(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 571 336**

(51) Int. CI.:

G06F 21/00 (2013.01)
H04L 29/08 (2006.01)
G06F 9/455 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.11.2011 E 11846297 (7)**

(97) Fecha y número de publicación de la concesión europea: **02.03.2016 EP 2570954**

(54) Título: **Método, dispositivo y sistema para prevenir un ataque de denegación de servicio distribuido en un sistema en la nube**

(30) Prioridad:

07.12.2010 CN 201010577221

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.05.2016

(73) Titular/es:

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

(72) Inventor/es:

JIANG, WU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, dispositivo y sistema para prevenir un ataque de denegación de servicio distribuido en un sistema en la nube

Campo de la invención

La presente invención está relacionada con el campo de las tecnologías informáticas y, en particular, con un método para prevenir ataques de Denegación de Servicio Distribuidos (DDOS) en un sistema en la nube, un nodo de protección en un sistema en la nube y un sistema de protección en un sistema en la nube.

Antecedentes de la invención

Un ataque de Denegación de Servicio Distribuido (DDOS) se refiere principalmente a un ataque en el que un atacante utiliza un servidor de control como un paso intermedio (pueden existir múltiples niveles y múltiples capas) y controla un gran número de servidores infectados y por lo tanto controlados para formar una red de ataque y lanzar ataques masivos de denegación de servicio sobre los servidores objetivo.

Los ataques de DDoS pueden utilizar la red de ataque para lanzar los ataques posteriores sobre los servidores objetivo, por ejemplo, un ataque por inundación del Protocolo de Mensajes de Control de Internet (ICMP), un ataque por inundación del Protocolo de Datagramas de Usuario (UDP), y un ataque por inundación de Sincronización (SYN). El ataque de DDoS normalmente amplifica de forma exponencial el ataque de un único atacante, provocando de este modo un impacto significativo sobre un servidor de usuario o incluso provocando un fallo del servidor de usuario, y provocando una grave congestión en la red.

En la actualidad, utilizando software de máquinas virtuales, sobre un ordenador físico se pueden simular una o más máquinas virtuales. Las máquinas virtuales funcionan como los ordenadores físicos. Por ejemplo, sobre las máquinas virtuales se pueden instalar los sistemas operativos y las aplicaciones, y las máquinas virtuales pueden acceder a los recursos de red. Las aplicaciones que se ejecutan en una máquina virtual funcionan como en un ordenador físico.

Un sistema de computación en la nube (un sistema en la nube para abreviar) se puede considerar como un sistema agrupado que realiza computación, almacenamiento y gestión distribuidos sobre un hardware universal. El sistema en la nube proporciona acceso a datos de alto rendimiento, y es aplicable a la computación y el almacenamiento de datos masivos.

Con el desarrollo de la tecnología del sistema en la nube, un sistema en la nube puede incluir decenas de miles de máquinas virtuales, y por lo tanto la protección de seguridad de las máquinas virtuales del sistema en la nube atrae más y más atención. Es especialmente importante prevenir los ataques de DDoS entre las máquinas virtuales del sistema en la nube. Sin embargo, un mecanismo para prevenir la DDoS existente consiste principalmente en prevenir los ataques de DDoS entre diferentes sistemas en la nube, entre un sistema en la nube y los servidores fuera del sistema en la nube, y entre los servidores entre sistemas que no se encuentran en la nube, pero no es aplicable para prevenir los ataques de DDoS entre máquinas virtuales de un sistema en la nube.

La solicitud de patente de los EE.UU. con número de publicación 2010/0269171 A1 divulga los pasos de un proceso para el flujo de paquetes desde una máquina virtual a otra. Cuando se envía un paquete desde una VM A a una VM B (Paso 20), el paquete es interceptado por un agente de seguridad A1, y se inyecta en un agente de seguridad remoto C1 (Paso 22). El agente de seguridad C1 reenvía el paquete a la VM C de seguridad (Paso 24). La VM C de seguridad inspecciona el paquete (Paso 26) y determina si el paquete está permitido (Paso 28). El paquete se descarta si no está permitido (Paso 30). Si el paquete está permitido, el paquete se etiqueta como “aprobado por seguridad” (Paso 32).

La solicitud de patente de los EE.UU. con número de publicación 2008/0163370 A1 divulga métodos y equipos que permiten que un analizador de tráfico monitorice una conexión interna de un sistema informático en busca de uno o más patrones de tráfico. El analizador de tráfico compara el tráfico sobre la conexión interna con un patrón de tráfico esperado, y lleva a cabo una acción basada en políticas teniendo en cuenta el resultado de la comparación entre el patrón de tráfico y el patrón esperado. El analizador de tráfico puede existir en una pila de una VMM o una VM de monitorización o se puede implementar en un motor de gestión del sistema informático.

La solicitud de patente de los EE.UU. con número de publicación 2009/0254990 A1 divulga un sistema de seguridad distribuido y coordinado que proporciona detección de intrusiones y prevención de intrusiones para las máquinas virtuales (VM) en un servidor virtual. La plataforma de virtualización del servidor virtual se mejora con los controladores de red que proporcionan una función de cortafuegos de “ruta rápida” para las VM huéspedes configuradas previamente que ya tienen instalados agentes de seguridad de inspección profunda de paquetes dedicados. Se despliega una VM de seguridad independiente para proporcionar agentes de seguridad virtuales

que proporcionen una inspección profunda de paquetes para las VM huéspedes no configuradas previamente. Los controladores de red se configuran entonces para interceptar el tráfico de datos de estas VM huéspedes y encaminarlas a través de sus agentes virtuales de seguridad correspondientes, proporcionando de este modo una “ruta lenta” para la detección y prevención de intrusiones.

Resumen de la invención

Los modos de realización de la presente invención proporcionan un método, un equipo y un sistema para prevenir ataques de DDoS en un sistema en la nube que prevengan de forma efectiva ataques de DDoS entre máquinas virtuales en un sistema en la nube.

Con el fin de resolver el problema técnico descrito más arriba, los modos de realización de la presente invención proporcionan las siguientes soluciones técnicas:

Un método para prevenir ataques de DDoS en un sistema en la nube incluye:

monitorizar, por parte de un nodo de protección en un sistema en la nube, el tráfico de datos de entrada de una máquina virtual, en donde el sistema en la nube incluye el nodo de protección y múltiples máquinas virtuales, y los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección;

extraer los flujos de datos que van a entrar en la máquina virtual si se detecta que el tráfico de datos de entrada de la máquina virtual es anormal;

enviar a un equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza;

recibir los flujos de datos limpios devueltos por el equipo de limpieza de tráfico; e

introducir en la máquina virtual los flujos de datos limpios;

en donde la monitorización del tráfico de datos de entrada de la máquina virtual comprende:

recoger estadísticas del tráfico de datos de entrada de la máquina virtual durante un tiempo fijado con antelación; y si las estadísticas muestran que el tráfico de datos de entrada de la máquina virtual dentro del tiempo fijado con antelación excede un umbral fijado con antelación, determinar que el tráfico de datos de entrada de la máquina virtual es anormal.

En un modo de realización de la presente invención se proporciona un nodo de protección en un sistema en la nube, en donde el sistema en la nube incluye el nodo de protección y múltiples máquinas virtuales, los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección, y el nodo de protección incluye:

un módulo de monitorización, configurado para monitorizar el tráfico de datos de entrada de una máquina virtual;

un módulo de extracción y envío, configurado para extraer los flujos de datos que van a entrar en la máquina virtual si se detecta que el tráfico de datos de entrada de la máquina virtual es anormal, y enviar a un equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza;

un módulo de recepción, configurado para recibir los flujos de datos limpios devueltos por el equipo de limpieza de tráfico; y

un módulo de introducción, configurado para introducir en la máquina virtual los flujos de datos limpios que han sido recibidos por el módulo de recepción;

en donde el módulo de monitorización está configurado específicamente para recoger estadísticas del tráfico de datos de entrada de la máquina virtual durante un tiempo fijado con antelación; y si las estadísticas muestran que el tráfico de datos de entrada de la máquina virtual dentro del tiempo fijado con antelación excede un umbral fijado con antelación, determinar que el tráfico de datos de entrada de la máquina virtual es anormal.

En un modo de realización de la presente invención se proporciona un sistema de protección en un sistema en la nube, en donde el sistema en la nube incluye un nodo de protección y múltiples máquinas virtuales, los flujos de datos que se transmiten entre máquinas virtuales pasan a través del nodo de protección, y el sistema de protección incluye:

un nodo de protección en un sistema en la nube, configurado para recoger estadísticas sobre el tráfico de datos de entrada de una máquina virtual dentro de un tiempo fijado con antelación; si las estadísticas muestran que el tráfico de datos de entrada de la máquina virtual dentro del tiempo fijado con antelación excede un umbral fijado con antelación, determinar que el tráfico de datos de entrada de la máquina virtual es anormal; extraer los flujos

de datos a introducir en la máquina virtual si se detecta que el tráfico de datos de entrada en la máquina virtual es anormal, y enviar a un equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; recibir los flujos de datos limpios por parte del equipo de limpieza de tráfico; e introducir los flujos de datos limpios en la máquina virtual; y

un equipo de limpieza de tráfico, configurado para limpiar los flujos de datos que provienen del nodo de protección en el sistema en la nube y que se van a introducir en la máquina virtual, y enviarle al nodo de protección en el sistema en la nube los flujos de datos limpios.

De este modo, en los modos de realización de la presente invención, en el sistema en la nube se despliega un nodo de protección. El nodo de protección en el sistema en la nube monitoriza el tráfico de datos de entrada de las máquinas virtuales; extrae los flujos de datos que se van a introducir en las máquinas virtuales si se detecta que el tráfico de datos de entrada de las máquinas virtuales es anormal, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; e introduce en las máquinas virtuales los flujos de datos limpios devueltos por el equipo de limpieza de tráfico. Como la protección de DDoS se lleva a cabo utilizando el nodo de protección en el sistema en la nube, se previenen no solamente los ataques de DDoS lanzados por redes externas sobre las máquinas virtuales del sistema en la nube, sino que también se previenen de forma efectiva los ataques de DDoS entre las máquinas virtuales del sistema en la nube, y se mejora de forma exhaustiva la seguridad y fiabilidad del sistema en la nube.

Breve descripción de los dibujos

Con el fin de ilustrar con más claridad las soluciones técnicas de los modos de realización de la presente invención o de la técnica anterior, a continuación se describen brevemente los dibujos adjuntos necesarios para describir los modos de realización o la técnica anterior. Evidentemente, los dibujos adjuntos de la siguiente descripción únicamente muestran algunos modos de realización de la presente invención, y las personas experimentadas en la técnica pueden derivar sin esfuerzos creativos otros dibujos a partir de estos dibujos.

La FIG. 1-a es un diagrama esquemático de un entorno virtual Xen de acuerdo con un modo de realización de la presente invención;

la FIG. 1-b es un diagrama esquemático de la estructura de un controlador del Dominio 0 de acuerdo con un modo de realización de la presente invención;

la FIG. 1-c es un diagrama esquemático de la estructura de un controlador del Dominio U de acuerdo con un modo de realización de la presente invención;

la FIG. 1-d es un diagrama esquemático de un proceso del Dominio 0 que protege el Dominio U de acuerdo con un modo de realización de la presente invención;

la FIG. 2 es un diagrama esquemático de ataques de DDoS de acuerdo con un modo de realización de la presente invención;

la FIG. 3 es un diagrama de flujo de un método para prevenir ataques de DDoS en un sistema en la nube de acuerdo con el Modo de realización 1 de la presente invención;

la FIG. 4 es un diagrama de flujo de un método para prevenir ataques de DDoS en un sistema en la nube de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 5-a es un diagrama esquemático de un nodo de protección en un sistema en la nube de acuerdo con el Modo de realización 3 de la presente invención;

la FIG. 5-b es un diagrama esquemático de otro nodo de protección en un sistema en la nube de acuerdo con el Modo de realización 3 de la presente invención; y

la FIG. 6 es un diagrama esquemático de un sistema de protección en un sistema en la nube de acuerdo con el Modo de realización 4 de la presente invención.

Descripción detallada de los modos de realización

Con el fin de hacer más comprensibles las soluciones técnicas de la presente invención para las personas experimentadas en la técnica, a continuación se describen de forma clara y completa las soluciones técnicas de acuerdo con los modos de realización de la presente invención haciendo referencia a los dibujos adjuntos en los modos de realización de la presente invención. Evidentemente, los modos de realización de la siguiente descripción son únicamente una parte en lugar de todos los modos de realización de la presente invención. Todos los demás modos de realización obtenidos sin esfuerzo creativo por personas experimentadas en la técnica a partir de los modos de realización de la presente invención se considerarán dentro del alcance de

protección de la presente invención.

Para facilitar la comprensión, a continuación se describe primero brevemente una forma de funcionamiento de un sistema virtual.

Tal como se muestra en la FIG. 1-a, un entorno virtual Xen puede incluir los siguientes elementos mutuamente colaborativos:

Hipervisor (monitor de máquina virtual) Xen

Dominio 0

Sistema de cliente PV del Dominio U

Sistema de cliente HVM del Dominio U

El Hipervisor Xen es una capa de software entre el hardware y el sistema operativo, y es principalmente responsable de la planificación de la unidad central de procesamiento (CPU) y del reparto de memoria entre las máquinas virtuales. El Hipervisor Xen no es únicamente responsable de abstraer la capa de hardware sino que también controla la ejecución de las máquinas virtuales ya que las máquinas virtuales comparten el mismo entorno de procesamiento. En general, el Hipervisor Xen no gestiona peticiones de red, peticiones de dispositivos de almacenamiento, peticiones de vídeo ni peticiones de Entrada/Salida (E/S).

El Dominio 0 es, en general, un núcleo de Linux modificado (u otro núcleo). El Dominio 0 se puede considerar como un nodo de gestión de otras máquinas virtuales. El Dominio 0 es en general una máquina virtual que se ejecuta exclusivamente sobre el Hipervisor Xen, y en general tiene permiso para acceder a los recursos físicos de E/S, e interactúa con otras máquinas virtuales que se ejecutan sobre un sistema virtual. El Dominio 0 se tiene que iniciar antes de que se inicien otros Dominios. El Dominio 0 incluye, en general, dos controladores (tal como se muestra en la FIG. 1-b): un Controlador Intermediario de Red y un Controlador Intermediario de Bloques, los cuales son responsables de gestionar las peticiones de red desde un Dominio U y las peticiones de disco local, respectivamente. El Controlador Intermediario de Red se puede comunicar directamente con el hardware de red local para gestionar todas las peticiones de red procedentes de un sistema operativo cliente sobre el Dominio U. El Controlador Intermediario de Bloques se puede comunicar con un dispositivo de almacenamiento local para gestionar las peticiones de lectura/escritura del Dominio U.

El Dominio U es una máquina virtual que se ejecuta sobre el Hipervisor Xen. Las máquinas virtuales completamente virtualizadas se denominan “Huéspedes HVM del Dominio U”, sobre las que se ejecuta un sistema operativo con un núcleo sin modificar (por ejemplo Windows); las máquinas virtuales paravirtualizadas se denominan “Huéspedes PV del dominio U”, sobre las que se ejecuta un sistema operativo con un núcleo modificado (por ejemplo Linux, Solaris, FreeBSD u otros sistemas operativos).

Los Huéspedes PV del dominio U también pueden incluir dos controladores (tal como se muestra en la FIG. 1-c): un controlador de red paravirtualizado (PV Network Driver), y un controlador de bloques paravirtualizado (PV Block Driver).

En las máquinas virtuales de los Huéspedes HVM del Dominio U existe un controlador no paravirtualizado (PV Driver), pero en el Dominio 0 se inicia un proceso demonio especial denominado Qemu-dm para cada uno de los clientes completamente virtualizados (HVM Guest), y el Qemu-dm es responsable de gestionar las peticiones de red y las peticiones de disco del sistema operativo cliente.

Tal como se muestra en la FIG. 1-d, los Huéspedes HVM del Dominio U se pueden inicializar en un tipo de máquina, y en el Dominio U se puede añadir el firmware virtual Xen con el fin de simular la BIOS.

Tal como se muestra en la FIG. 2, un ataque de red sobre un sistema en la nube incluye principalmente tres tipos:

un ataque de red externo sobre un sistema en la nube, el cual es principalmente un ataque lanzado por una red externa;

un ataque entre diferentes servidores físicos en un sistemas en la nube, el cual es principalmente un ataque lanzado entre diferentes servidores físicos en un sistema en la nube; y

un ataque entre diferentes máquinas virtuales en el mismo servidor físico en un sistema en la nube, el cual es principalmente un ataque lanzado entre diferentes servidores virtuales en el mismo servidor físico en un sistema en la nube.

Los modos de realización de la presente invención tratan principalmente la protección contra ataques de

Denegación de Servicio Distribuidos (DDoS) lanzados entre diferentes máquinas virtuales sobre el mismo servidor físico o diferentes servidores físicos sobre un sistema en la nube.

A continuación se ofrecen más detalles sobre los modos de realización de la presente invención.

Modo de realización 1

Este modo de realización proporciona un método para prevenir los ataques de Denegación de Servicio Distribuidos (DDoS) en un sistema en la nube. El método puede incluir: monitorizar, por parte de un nodo de protección en un sistema en la nube, el tráfico de datos de entrada en las máquinas virtuales; extraer los flujos de datos a introducir en las máquinas virtuales si se detecta que el tráfico de datos de entrada en las máquinas virtuales es anormal, y enviarle a un equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; recibir los flujos de datos limpios devueltos por el equipo de limpieza de tráfico; e introducir los flujos de datos limpios en las máquinas virtuales.

Tal como se muestra en la FIG. 3, el método puede incluir los siguientes pasos detallados:

310. El nodo de protección en el sistema en la nube monitoriza el tráfico de datos de entrada en las máquinas virtuales.

El sistema en la nube incluye el nodo de protección y múltiples máquinas virtuales, y los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección.

En un escenario de aplicación, el nodo de protección en el sistema en la nube puede ser un nodo de gestión de máquinas virtuales en el sistema en la nube (el nodo de gestión de máquinas virtuales en el sistema en la nube gestiona una o más máquinas virtuales localizadas en el mismo servidor físico o en diferentes servidores físicos en el sistema en la nube), o puede ser un equipo desplegado entre el nodo de gestión de máquinas virtuales y cada una de las máquinas virtuales en el sistema en la nube. Los flujos de datos que se transmiten entre la red externa y cada una de las máquinas virtuales en el sistema en la nube, y los flujos de datos que se transmiten entre las máquinas virtuales en el sistema en la nube, pasan a través del nodo de protección en el sistema en la nube. El nodo de protección en el sistema en la nube monitoriza los flujos de datos a ser introducidos en las máquinas virtuales. Los flujos de datos de entrada de una máquina virtual pueden proceder de la red externa, o pueden proceder de otras máquinas virtuales en el sistema en la nube. La función de protección y la función de monitorización se pueden implementar mediante un software de protección de seguridad sobre el nodo de gestión de máquinas virtuales.

En una aplicación práctica, el nodo de protección en el sistema en la nube puede, por ejemplo, recoger estadísticas sobre el tráfico de datos de entrada de las máquinas virtuales dentro de un tiempo fijado con antelación (por ejemplo 30 segundos, 1 minuto u otro valor). Si las estadísticas muestran que el tráfico de datos de entrada en una máquina virtual dentro de un tiempo fijado con antelación excede un umbral fijado con antelación (por ejemplo 50 MB, 100 MB u otro valor), se puede determinar que el tráfico de datos de entrada en la máquina virtual es anormal.

320. Si el nodo de protección en el sistema en la nube detecta que el tráfico de datos de entrada en las máquinas virtuales es anormal, el nodo de protección extrae los flujos de datos a ser introducidos en las máquinas virtuales, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza.

En un escenario de aplicación, cuando el nodo de protección en el sistema en la nube detecta que el tráfico de datos de entrada en las máquinas virtuales es anormal, el nodo de protección en el sistema en la nube puede extraer directamente los flujos de datos a ser introducidos en las máquinas virtuales, y enviarle directamente al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza. Alternativamente, después de que el nodo de protección en el sistema en la nube haya detectado que el tráfico de datos de entrada en las máquinas virtuales es anormal, el nodo de protección puede enviar en primer lugar, al equipo de limpieza de tráfico, una petición de limpieza de tráfico que indica una petición para limpiar el tráfico; si desde el equipo de limpieza de tráfico se recibe una respuesta de limpieza de tráfico que indica el permiso para la limpieza del tráfico (indicando que el equipo de limpieza de tráfico dispone de suficientes recursos para la limpieza, en donde los recursos para la limpieza se pueden referir a capacidad de procesamiento sin utilizar), entonces el nodo de protección extrae los flujos de datos a ser introducidos en las máquinas virtuales, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza. Además, si desde el equipo de limpieza de tráfico se recibe una respuesta de limpieza de tráfico que indica que no existe permiso de limpieza de tráfico (indicando que el equipo de limpieza de tráfico no dispone en este momento de suficientes recursos para la limpieza), el nodo de protección en el sistema en la nube puede esperar cierto periodo (por ejemplo 2 segundos, 5 segundos u otro valor), y a continuación enviarle al equipo de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para la limpieza del tráfico. Este proceso se repite hasta que el equipo de limpieza de tráfico termina de limpiar tráfico. En particular, si se encuentran disponibles para su selección múltiples equipos de limpieza de tráfico, entonces si el equipo de limpieza de tráfico al que se le acaba de solicitar la limpieza del tráfico no

dispone de suficientes recursos para la limpieza en este momento, el nodo de protección en el sistema en la nube puede solicitarle a otro equipo de limpieza de tráfico que limpie el tráfico.

En una aplicación práctica, el tráfico de datos anormal puede ser causado por inundación UDP, inundación SYN, inundación ICMP, u otro ataque de DDoS. El iniciador del ataque de DDoS puede ser una red externa u otra máquina virtual en el sistema en la nube.

El equipo de limpieza de tráfico puede consistir en una placa de limpieza de tráfico desplegada de forma independiente, u otra estructura desplegada. El equipo de limpieza de tráfico puede limpiar el tráfico utilizando una o más de las siguientes tecnologías: salto SYN, proxy de TCP, limitación de flujo UDP, detección de conexiones inválidas, salto de TC de DNS y otras tecnologías de la técnica anterior.

330. El nodo de protección en el sistema en la nube recibe los flujos de datos limpios devueltos por el equipo de limpieza de tráfico.

340. El nodo de protección en el sistema en la nube introduce los flujos de datos limpios en las máquinas virtuales.

Naturalmente, el nodo de protección en el sistema en la nube introduce los flujos de datos limpios devueltos por el equipo de limpieza de tráfico de vuelta en las máquinas virtuales correspondientes. De este modo, las máquinas virtuales pueden recibir los flujos de datos limpios y pueden responderlos y procesarlos normalmente.

A partir de lo descrito más arriba se puede observar que en este modo de realización en el sistema en la nube se despliega un nodo de protección. El nodo de protección en el sistema en la nube monitoriza el tráfico de datos de entrada de las máquinas virtuales; extrae los flujos de datos a ser introducidos en las máquinas virtuales si se detecta que el tráfico de datos de entrada de las máquinas virtuales es anormal, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; e introduce los flujos de datos limpios devueltos por el equipo de limpieza de tráfico de vuelta en las máquinas virtuales. Debido a que la protección de DDoS se lleva a cabo utilizando el nodo de protección en el sistema en la nube, se previenen no solamente los ataques de DDoS lanzados por redes externas sobre las máquinas virtuales en el sistema en la nube, sino que también se previenen de forma efectiva los ataques de DDoS entre las máquinas virtuales en el sistema en la nube, y de este modo se mejora de forma exhaustiva la seguridad y fiabilidad del sistema en la nube.

Modo de realización 2

Con el fin de facilitar una mejor comprensión de la solución técnica de la presente invención, a continuación se presentan más detalles tomando como ejemplo un proceso en el que un nodo de gestión de máquinas virtuales en un sistema en la nube protege contra ataques de DDoS a una máquina virtual Ai en el sistema en la nube.

Tal como se muestra en la FIG. 4, el proceso puede incluir:

401. El nodo de gestión de máquinas virtuales en el sistema en la nube monitoriza el tráfico de datos de entrada en la máquina virtual Ai.

En un escenario de aplicación, el nodo de gestión de máquinas virtuales en el sistema en la nube puede gestionar una o más máquinas virtuales (incluyendo la máquina virtual Ai) localizadas en el mismo servidor físico o en diferentes servidores físicos en el sistema en la nube.

Los flujos de datos que se transmiten entre la red externa y cada una de las máquinas virtuales en el sistema en la nube, y los flujos de datos que se transmiten entre las máquinas virtuales en el sistema en la nube, pasan a través del nodo de gestión de máquinas virtuales en el sistema en la nube. El nodo de gestión de máquinas virtuales en el sistema en la nube monitoriza los flujos de datos a ser introducidos en las máquinas virtuales. El tráfico de datos de entrada de una máquina virtual puede proceder de una red externa, o puede proceder de otras máquinas virtuales en el sistema en la nube.

Tal como se muestra en la FIG. 1-a, si se considera el Dominio 0 como un nodo de gestión de máquinas virtuales en el sistema en la nube, el Dominio U es una máquina virtual gestionada por el Dominio 0.

En una aplicación práctica, el nodo de gestión de máquinas virtuales en el sistema en la nube puede, por ejemplo, recoger estadísticas sobre el tráfico de datos de entrada de la máquina virtual Ai dentro de un tiempo fijado con antelación (por ejemplo 30 segundos, 1 minuto u otro valor). Si la máquina virtual Ai dispone de una dirección del Protocolo de Internet (IP), o una dirección del Control de Acceso al Medio (MAC) u otra dirección de salida, el nodo de gestión de máquinas virtuales en el sistema en la nube puede generar una tabla de monitorización en función de la dirección de destino del tráfico de datos con el fin de monitorizar el tráfico de datos de entrada de la máquina virtual Ai, y puede utilizar la tabla de monitorización para registrar la información estadística.

402. Si el nodo de gestión de máquinas virtuales en el sistema en la nube detecta que el tráfico de datos de entrada de la máquina virtual Ai es anormal, el nodo de gestión le envía al equipo de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para limpiar el tráfico.

Específicamente, si las estadísticas recogidas por el nodo de gestión de máquinas virtuales en el sistema en la nube muestran que el tráfico de datos de entrada en la máquina virtual Ai dentro de un tiempo fijado con antelación excede un umbral fijado con antelación (por ejemplo 50 MB, 100 MB u otro valor), el nodo de gestión determina que el tráfico de datos de entrada en la máquina virtual Ai es anormal e inicia un mecanismo de limpieza de tráfico. La petición de limpieza de tráfico puede incluir, además, un identificador de la máquina virtual Ai, y en consecuencia, el equipo de limpieza de tráfico puede saber que el tráfico de datos de entrada en la máquina virtual Ai es anormal.

403. El equipo de limpieza de tráfico le envía una respuesta de limpieza de tráfico al nodo de gestión de máquinas virtuales en el sistema en la nube.

En una aplicación práctica, el equipo de limpieza de tráfico puede detectar si en el momento de la petición existen suficientes recursos de limpieza (los recursos para la limpieza se pueden referir a capacidad de procesamiento sin utilizar), y, si en dicho momento existen suficientes recursos para la limpieza, enviarle al nodo de gestión de máquinas virtuales en el sistema en la nube una respuesta de limpieza de tráfico que indica permiso para la limpieza del tráfico (la respuesta de limpieza de tráfico puede seguir incluyendo el identificador de la máquina virtual Ai).

Sin embargo, cuando se detecta que en el momento de la petición no existen suficientes recursos, el equipo de limpieza de tráfico puede enviarle al nodo de gestión de máquinas virtuales en el sistema en la nube una respuesta de limpieza de tráfico que indica que en dicho momento no existe permiso para la limpieza del tráfico (la respuesta de limpieza de tráfico puede seguir incluyendo el identificador de la máquina virtual Ai) y, en consecuencia, el nodo de gestión de máquinas virtuales en el sistema en la nube puede esperar durante un tiempo específico (por ejemplo 2 segundos, 5 segundos u otro valor), y a continuación enviarle al equipo de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para la limpieza del tráfico. Este proceso se repite hasta que el equipo de limpieza de tráfico termina de limpiar tráfico. En particular, si se encuentran disponibles para su selección múltiples equipos de limpieza de tráfico, entonces si el equipo de limpieza de tráfico al que se le acaba de solicitar la limpieza del tráfico no dispone de suficientes recursos para la limpieza en este momento, el nodo de protección en el sistema en la nube puede solicitarle a otro equipo de limpieza de tráfico que limpie el tráfico.

Aquí, se toma como ejemplo un escenario en el que el equipo de limpieza de tráfico dispone de suficientes recursos de limpieza para la limpieza del tráfico de la máquina virtual Ai en el momento de la petición.

404. El nodo de gestión de máquinas virtuales en el sistema en la nube recibe del equipo de limpieza de tráfico una respuesta de limpieza de tráfico que indica que existe permiso para limpiar el tráfico, extrae los flujos de datos a ser introducidos en la máquina virtual Ai, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para limpiar el tráfico.

En una aplicación práctica, el tráfico de datos anormal puede ser causado por inundación UDP, inundación SYN, inundación ICMP, u otro ataque de DDoS. El iniciador del ataque de DDoS puede ser una red externa u otra máquina virtual en el sistema en la nube.

El equipo de limpieza de tráfico puede consistir en una placa de limpieza de tráfico desplegada de forma independiente, u otra estructura desplegada. El equipo de limpieza de tráfico puede limpiar el tráfico anormal de la máquina virtual Ai con el fin de eliminar tráfico sospechoso utilizando una o más de las siguientes tecnologías: salto SYN, proxy de TCP, limitación de flujo UDP, detección de conexiones inválidas, salto de TC de DNS y otras tecnologías de la técnica anterior.

Por ejemplo, si el equipo de limpieza de tráfico limpia el tráfico basándose en el mecanismo de salto SYN, cuando se recibe un paquete SYN desde un cliente a un servidor de destino, el equipo de limpieza de tráfico puede simular que es un servidor de destino para comunicarse con el cliente, y responder con un paquete SYN-ACK construido especialmente con un número de serie de confirmación. Si la IP origen del cliente en el paquete SYN es real, el cliente recibe un paquete SYN-ACK especial enviado por el equipo de limpieza de tráfico, y al mismo tiempo construye un paquete RST que tiene el mismo número de serie como número de serie de confirmación original. El equipo de limpieza de tráfico realiza una comprobación en función de la información del paquete. Si el número de serie es el mismo que el número de serie del paquete SYN-ACK creado inicialmente, el equipo de limpieza de tráfico considera la IP como real, y añade la IP a una lista blanca. Posteriormente, el cliente vuelve a enviar el paquete SYN de forma automática, y el equipo de limpieza de tráfico recibe el paquete y puede reenviar el paquete directamente si el equipo de limpieza de tráfico lo encuentra en la lista blanca.

Si el equipo de limpieza de tráfico limpia el tráfico basándose en un mecanismo de proxy TCP, cuando llega un

paquete SYN desde un cliente al equipo de limpieza de tráfico, un proxy SYN no reenvía el paquete SYN, sino que le devuelve al cliente un paquete SYN-ACK de forma proactiva en nombre de un servidor. Si desde el cliente se recibe un paquete ACK, ello indica que el acceso es normal, y el equipo de limpieza de tráfico le envía al servidor un paquete SYN y completa la negociación a tres vías, y a continuación se comunica con el servidor y el cliente en nombre del cliente y el servidor, respectivamente, con el fin de completar el reenvío.

Si el equipo de limpieza de tráfico limpia el tráfico basándose en un mecanismo de limitación de UDP actual, cuando el tráfico excede un umbral, el equipo de limpieza de tráfico limita el tráfico con el propósito de protección.

Si el equipo de limpieza de tráfico limpia el tráfico basándose en una detección de conexiones inválidas, el equipo de limpieza de tráfico puede recoger estadísticas de forma periódica sobre el número de conexiones TCP de una IP que se encuentra protegida y, una vez que un valor de las estadísticas excede un umbral, determina que se está produciendo un ataque de conexiones inválidas, y restringe una IP de origen desde la que se están iniciando demasiadas conexiones TCP.

Si el equipo de limpieza de tráfico limpia el tráfico basándose en un mecanismo de salto de TC de DNS, el equipo de limpieza de tráfico puede resolver el problema de la protección de seguridad de la seguridad de DNS convirtiendo un modo de comunicación UDP del DNS en un modo de comunicación TCP, mejorando de este modo en gran medida la capacidad de protección de seguridad del DNS. El DNS dispone de la siguiente funcionalidad: cuando el cliente envía una petición, si un servidor de DNS está preparado para devolver una respuesta pero descubre que la cantidad de datos es demasiado grande, que es mayor de que 512 bytes, el servidor de DNS asigna el valor 1 al indicador TC en el campo Flag (Indicador) de la cabecera del paquete DNS, y a continuación le devuelve al cliente los 512 bytes de datos truncados. Después de recibir el paquete, el encargado de resolver los nombres de dominio del cliente lee en primer lugar el campo TC, y comprueba que el paquete está truncado y, por lo tanto, utiliza un modo de conexión TCP para conectarse al puerto TCP del DNS de forma proactiva, y envía de nuevo la petición para intercambiar la información.

Naturalmente, los mecanismos de limpieza de tráfico utilizados por el equipo de limpieza de tráfico no se encuentran limitados a los mecanismos de limpieza de tráfico descritos más arriba. El equipo de limpieza de tráfico puede utilizar otros modos de limpieza de tráfico para limpiar el tráfico según las necesidades.

405. El equipo de limpieza de tráfico le envía el tráfico de datos limpio al nodo de gestión de máquinas virtuales en el sistema en la nube.

406. El nodo de gestión de máquinas virtuales en el sistema en la nube recibe los flujos de datos limpios del equipo de limpieza de tráfico, e introduce los flujos de datos limpios en la máquina virtual Ai.

Naturalmente, el nodo de gestión de máquinas virtuales en el sistema en la nube introduce los flujos de datos limpios devueltos por el equipo de limpieza de tráfico de vuelta en la máquina virtual Ai. De este modo, la máquina virtual Ai puede recibir los flujos de datos limpios y también puede responder y procesarlos normalmente, evitando de este modo que una red externa u otras máquinas virtuales en el sistema en la nube lancen ataques de DDoS sobre la máquina virtual Ai.

Por lo tanto, en este modo de realización, el nodo de gestión de máquinas virtuales en el sistema en la nube monitoriza el tráfico de datos de entrada de las máquinas virtuales; extrae los flujos de datos a ser introducidos en una máquina virtual si se detecta que el tráfico de datos de entrada de la máquina virtual es anormal, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; e introduce los flujos de datos limpios devueltos por el equipo de limpieza de tráfico de vuelta en la máquina virtual. Debido a que la protección de DDoS se lleva a cabo utilizando el nodo de protección en el sistema en la nube, se previenen no solamente los ataques de DDoS lanzados por redes externas sobre las máquinas virtuales en el sistema en la nube, sino que también se previenen de forma efectiva los ataques de DDoS entre las máquinas virtuales en el sistema en la nube, y de este modo se mejora de forma exhaustiva la seguridad y fiabilidad del sistema en la nube.

Con el fin de implementar mejor la solución técnica de la presente invención descrita más arriba, a continuación se describen un equipo y un sistema para implementar la solución técnica anterior descrita más arriba.

Modo de realización 3

Tal como se muestra en la FIG. 5, este modo de realización proporciona un nodo 500 de protección en un sistema en la nube, en donde el sistema en la nube incluye el nodo de protección y múltiples máquinas virtuales, los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección, y el nodo 500 de protección en el sistema en la nube puede incluir específicamente: un módulo 510 de monitorización, un módulo 520 de extracción y envío, un módulo 530 de recepción, y un módulo 540 de introducción. El módulo 510 de monitorización está configurado para monitorizar el tráfico de datos de entrada en las máquinas virtuales.

En un escenario de aplicación, el nodo 500 de protección en el sistema en la nube puede ser un nodo de gestión de máquinas virtuales en el sistema en la nube (el nodo de gestión de máquinas virtuales en el sistema en la nube gestiona una o más máquinas virtuales localizadas en el mismo servidor físico o en diferentes servidores físicos en el sistema en la nube), o puede ser un equipo desplegado entre el nodo de gestión de máquinas virtuales y cada una de las máquinas virtuales en el sistema en la nube. Los flujos de datos que se transmiten entre la red externa y cada una de las máquinas virtuales en el sistema en la nube, y los flujos de datos que se transmiten entre las máquinas virtuales en el sistema en la nube, pasan a través del nodo 500 de protección en el sistema en la nube. El nodo 500 de protección en el sistema en la nube monitoriza los flujos de datos a ser introducidos en las máquinas virtuales. Los flujos de datos de entrada de una máquina virtual pueden proceder de la red externa, o pueden proceder de otras máquinas virtuales en el sistema en la nube.

El módulo 510 de monitorización está configurado específicamente para recoger estadísticas sobre el tráfico de datos de entrada de las máquinas virtuales dentro de un tiempo fijado con antelación (por ejemplo 30 segundos, 1 minuto u otro valor); si las estadísticas muestran que el tráfico de datos de entrada en la máquina virtual dentro de un tiempo fijado con antelación excede un umbral fijado con antelación (por ejemplo 50 MB, 100 MB u otro valor), se determina que el tráfico de datos de entrada en la máquina virtual es anormal.

El módulo 520 de extracción y envío está configurado para extraer los flujos de datos a ser introducidos en las máquinas virtuales si el módulo 510 de monitorización detecta que el tráfico de datos de entrada en las máquinas virtuales es anormal, y enviarle al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza.

El módulo 530 de recepción está configurado para recibir los flujos de datos limpios devueltos por el equipo de limpieza de tráfico.

El módulo 540 de introducción está configurado para introducir en las máquinas virtuales los flujos de datos limpios que han sido recibidos por el módulo 530 de recepción.

Tal como se muestra en la FIG. 5-b, en un escenario de aplicación, el nodo 500 de protección en el sistema en la nube puede incluir, además:

un módulo 550 de petición, configurado para: antes de que el módulo 520 de extracción y envío extraiga los flujos de datos a ser introducidos en las máquinas virtuales, enviarle al equipo de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para limpiar el tráfico; y

un módulo 560 de respuesta, configurado para recibir una respuesta de limpieza de tráfico desde el equipo de limpieza de tráfico, en donde la respuesta de limpieza de tráfico indica permiso para limpiar el tráfico.

Se debe observar que el nodo 500 de protección en el sistema en la nube en este modo de realización puede ser un nodo de gestión de máquinas virtuales en el sistema en la nube del modo de realización anterior, y puede servir para colaborar en la implementación de todas las soluciones técnicas en los modos de realización del método descritos más arriba. Las funciones de los módulos de función del nodo de protección se pueden implementar de acuerdo con los métodos descritos en los modos de realización del método descritos más arriba. Para el proceso de implementación detallado se puede hacer referencia a las descripciones apropiadas en los modos de realización descritos más arriba.

A partir de la descripción anterior se puede observar que, en este modo de realización, el nodo de protección se despliega en el sistema en la nube. El nodo 500 de protección en el sistema en la nube monitoriza el tráfico de datos de entrada de las máquinas virtuales; extrae los flujos de datos a ser introducidos en las máquinas virtuales si se detecta que el tráfico de datos de entrada de las máquinas virtuales es anormal, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; e introduce los flujos de datos limpios devueltos por el equipo de limpieza de tráfico de vuelta en las máquinas virtuales. Debido a que la protección de DDoS se lleva a cabo utilizando el nodo de protección en el sistema en la nube, se previenen no solamente los ataques de DDoS lanzados por redes externas sobre las máquinas virtuales en el sistema en la nube, sino que también se previenen de forma efectiva los ataques de DDoS entre las máquinas virtuales en el sistema en la nube, y de este modo se mejora de forma exhaustiva la seguridad y fiabilidad del sistema en la nube.

Modo de realización 4

La FIG. 6 es un diagrama esquemático de un sistema de protección en un sistema en la nube de acuerdo con un modo de realización de la presente invención. El sistema en la nube incluye un nodo de protección y múltiples máquinas virtuales, los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección, y el sistema de protección puede incluir un nodo 610 de protección en el sistema en la nube y un equipo 620 de limpieza de tráfico.

El nodo 610 de protección en el sistema en la nube está configurado para monitorizar el tráfico de datos de entrada en las máquinas virtuales; extraer los flujos de datos a introducir en las máquinas virtuales si se detecta

que el tráfico de datos de entrada en las máquinas virtuales es anormal, y enviarle a un equipo 620 de limpieza de tráfico los flujos de datos extraídos para su limpieza; recibir los flujos de datos limpios devueltos por el equipo 620 de limpieza de tráfico; e introducir en las máquinas virtuales los flujos de datos limpios devueltos por el equipo 620 de limpieza de tráfico.

El equipo 620 de limpieza de tráfico está configurado para limpiar los flujos de datos procedentes del nodo 610 de protección en el sistema en la nube y que se van a introducir en las máquinas virtuales, y para enviarle los flujos de datos limpios al nodo 610 de protección en el sistema en la nube.

En un escenario de aplicación, el nodo 610 de protección en el sistema en la nube puede ser un nodo de gestión de máquinas virtuales en el sistema en la nube (el nodo de gestión de máquinas virtuales en el sistema en la nube gestiona una o más máquinas virtuales localizadas en el mismo servidor físico o en diferentes servidores físicos en el sistema en la nube), o puede ser un equipo desplegado entre el nodo de gestión de máquinas virtuales y cada una de las máquinas virtuales en el sistema en la nube. Los flujos de datos que se transmiten entre la red externa y cada una de las máquinas virtuales en el sistema en la nube, y los flujos de datos que se transmiten entre las máquinas virtuales en el sistema en la nube, pasan a través del nodo 610 de protección en el sistema en la nube. El nodo 610 de protección en el sistema en la nube monitoriza los flujos de datos a ser introducidos en las máquinas virtuales. Los flujos de datos de entrada de una máquina virtual pueden proceder de una red externa, o pueden proceder de otras máquinas virtuales en el sistema en la nube.

En una aplicación práctica, el nodo 610 de protección en el sistema en la nube puede, por ejemplo, recoger estadísticas sobre el tráfico de datos de entrada de las máquinas virtuales dentro de un tiempo fijado con antelación (por ejemplo 30 segundos, 1 minuto u otro valor). Si las estadísticas muestran que el tráfico de datos de entrada en las máquinas virtuales dentro de un tiempo fijado con antelación excede un umbral fijado con antelación (por ejemplo 50 MB, 100 MB u otro valor), se puede determinar que el tráfico de datos de entrada en las máquinas virtuales es anormal.

En un escenario de aplicación, cuando el nodo 610 de protección en el sistema en la nube detecta que el tráfico de datos de entrada de las máquinas virtuales es anormal, el nodo 610 de protección en el sistema en la nube puede extraer directamente los flujos de datos a ser introducidos en las máquinas virtuales, y enviarle directamente al equipo 620 de limpieza de tráfico los flujos de datos extraídos para su limpieza. Alternativamente, después de que el nodo 610 de protección haya detectado que el tráfico de datos de entrada en las máquinas virtuales es anormal, el nodo de protección puede enviar en primer lugar, al equipo 620 de limpieza de tráfico, una petición de limpieza de tráfico que indica una petición para limpiar el tráfico; después de haber recibido una respuesta de limpieza de tráfico que indica permiso para la limpieza del tráfico desde el equipo 620 de limpieza de tráfico (indicando que el equipo 620 de limpieza de tráfico dispone de suficientes recursos para la limpieza), el nodo de protección extrae los flujos de datos a ser introducidos en las máquinas virtuales, y le envía al equipo 620 de limpieza de tráfico los flujos de datos extraídos para su limpieza. Además, si desde el equipo 620 de limpieza de tráfico se recibe una respuesta de limpieza de tráfico que indica que no existe permiso de limpieza de tráfico (indicando que el equipo 620 de limpieza de tráfico puede no disponer en este momento de suficientes recursos para la limpieza), el nodo 610 de protección en el sistema en la nube puede esperar un tiempo específico (por ejemplo 2 segundos, 5 segundos u otro valor), y a continuación enviarle al equipo 620 de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para limpieza de tráfico. Este proceso se repite hasta que el equipo 620 de limpieza de tráfico termina de limpiar tráfico.

En particular, si se encuentran disponibles para su selección múltiples equipos de limpieza de tráfico, entonces si el equipo 620 de limpieza de tráfico al que se le acaba de solicitar la limpieza del tráfico no dispone de suficientes recursos para la limpieza en este momento, el nodo 610 de protección en el sistema en la nube puede solicitarle a otro equipo de limpieza de tráfico que limpie el tráfico.

En una aplicación práctica, el tráfico de datos anormal puede ser causado por inundación UDP, inundación SYN, inundación ICMP, u otro ataque de DDoS. El iniciador del ataque de DDoS puede ser una red externa u otra máquina virtual en el sistema en la nube.

El equipo 620 de limpieza de tráfico puede consistir en una placa de limpieza de tráfico desplegada de forma independiente, u otra estructura desplegada. El equipo 620 de limpieza de tráfico puede limpiar el tráfico utilizando una o más de las siguientes tecnologías: salto SYN, proxy de TCP, limitación de flujo UDP, detección de conexiones inválidas, salto de TC de DNS y/o una o más entre otras tecnologías de la técnica anterior.

Se debe observar que, por brevedad, los modos de realización del método anteriores se describen como una serie de acciones. Pero aquellos experimentados en la técnica deberían entender que la presente invención no se encuentra limitada por el orden de las acciones descritas, ya que de acuerdo con la presente invención, algunos pasos pueden adoptar otro orden o ejecutarse simultáneamente. Además, las personas experimentadas en la técnica deberían entender que todos los modos de realización descritos son ejemplos de modos de realización, y las acciones y módulos involucrados no son necesariamente requeridos por la presente invención.

En los modos de realización, la descripción de cada uno de los modos de realización destaca un aspecto, y para algunos modos de realización que pueden no haberse detallado se puede hacer referencia a la descripción pertinente de otros modos de realización.

En conjunto, en los modos de realización de la presente invención, se despliega un nodo de protección en el sistema en la nube. El nodo de protección en el sistema en la nube monitoriza el tráfico de datos de entrada de las máquinas virtuales; extrae los flujos de datos a ser introducidos en las máquinas virtuales si se detecta que el tráfico de datos de entrada de las máquinas virtuales es anormal, y le envía al equipo de limpieza de tráfico los flujos de datos extraídos para su limpieza; e introduce los flujos de datos limpios devueltos por el equipo de limpieza de tráfico de vuelta en las máquinas virtuales. Debido a que la protección de DDoS se lleva a cabo utilizando el nodo de protección en el sistema en la nube, se previenen no solamente los ataques de DDoS lanzados por redes externas sobre las máquinas virtuales en el sistema en la nube, sino que también se previenen de forma efectiva los ataques de DDoS entre las máquinas virtuales en el sistema en la nube, y de este modo se mejora de forma exhaustiva la seguridad y fiabilidad del sistema en la nube.

Las personas experimentadas en la técnica deberían entender que todos o parte de los pasos de los métodos en los modos de realización se pueden implementar mediante un programa que controle el hardware apropiado. El programa se puede encontrar almacenado en un medio de almacenamiento legible por un ordenador como, por ejemplo, una memoria de sólo lectura, una memoria de acceso aleatorio, un disco magnético o un disco óptico.

El texto anterior expone un método, un equipo y un sistema para prevenir los ataques de denegación de servicio distribuidos en un sistema en la nube de acuerdo con los modos de realización de la presente invención. Aunque la invención se describe haciendo referencia a algunos ejemplos de modos de realización, la invención no se encuentra limitada a dichos modos de realización. Es evidente que aquellos experimentados en la técnica pueden realizar modificaciones y variaciones a la invención sin apartarse de la idea y alcance de la invención. La invención pretende cubrir las modificaciones y variaciones proporcionadas que se encuentran dentro del alcance de protección definido por las siguientes reivindicaciones o sus equivalentes.

REIVINDICACIONES

1. Un método para prevenir los ataques de denegación de servicio distribuidos en un sistema en la nube, que comprende:

monitorizar (310, 410), por parte de un nodo de protección en un sistema en la nube, el tráfico de datos de entrada en una máquina virtual, en donde el sistema en la nube comprende el nodo de protección y múltiples máquinas virtuales, y los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección;

extraer (320, 404) los flujos de datos a ser introducidos en la máquina virtual si se detecta que el tráfico de datos de entrada en la máquina virtual es anormal;

enviar (320, 404) los flujos de datos extraídos a un equipo de limpieza de tráfico para su limpieza;

recibir (330, 405) los flujos de datos limpios devueltos por el equipo de limpieza de tráfico; e

introducir (340, 406) los flujos de datos limpios en la máquina virtual;

en donde la monitorización (310, 410) del tráfico de datos de entrada en la máquina virtual comprende:

recoger estadísticas sobre el tráfico de datos de entrada en la máquina virtual dentro de un tiempo fijado con antelación; y

si las estadísticas muestran que el tráfico de datos de entrada en la máquina virtual dentro del tiempo fijado con antelación excede un umbral fijado con antelación, determinar que el tráfico de datos de entrada en la máquina virtual es anormal.

2. El método de acuerdo con al reivindicación 1, en donde:

el nodo de protección en el sistema en la nube comprende un nodo de gestión de máquinas virtuales en el sistema en la nube.

3. El método de acuerdo con la reivindicación 1 ó 2, en donde:

antes de extraer el tráfico de datos a ser introducido en la máquina virtual, el método comprende, además:

enviarle al equipo de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para la limpieza del tráfico; y

recibir desde el equipo de limpieza de tráfico una respuesta de limpieza de tráfico que indica el permiso para la limpieza del tráfico.

4. Un nodo de protección en un sistema en la nube, en donde el sistema en la nube comprende el nodo de protección y múltiples máquinas virtuales, los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección, y el nodo de protección comprende:

un módulo (510) de monitorización, configurado para monitorizar el tráfico de datos de entrada en una máquina virtual;

un módulo (520) de extracción y envío, configurado para extraer los flujos de datos a ser introducidos en la máquina virtual si el módulo de monitorización detecta que el tráfico de datos de entrada en la máquina virtual es anormal, y enviarle los flujos de datos extraídos a un equipo de limpieza de tráfico para su limpieza;

un módulo (530) de recepción, configurado para recibir los flujos de datos limpios devueltos por el equipo de limpieza de tráfico; y

un módulo (540) de introducción, configurado para introducir los flujos de datos limpios que ha recibido el módulo de recepción en la máquina virtual;

en donde el módulo (510) de monitorización está configurado específicamente para recoger estadísticas sobre el tráfico de datos de entrada en la máquina virtual dentro de un tiempo fijado con antelación; si las estadísticas muestran que el tráfico de datos de entrada en la máquina virtual dentro del tiempo fijado con antelación excede un umbral fijado con antelación, determinar que el tráfico de datos de entrada en la máquina virtual es anormal.

5. El nodo de protección de acuerdo con la reivindicación 4, en donde:

el nodo de protección comprende un nodo de gestión de máquinas virtuales en el sistema en la nube.

6. El nodo de protección de acuerdo con la reivindicación 4 ó 5, que comprende, además:

un módulo (550) de petición, configurado para: antes de que el módulo de extracción y envío extraiga los flujos de datos a ser introducidos en la máquina virtual, enviarle al equipo de limpieza de tráfico una petición de limpieza de tráfico que indica una petición para la limpieza del tráfico; y

un módulo (560) de respuesta, configurado para recibir desde el equipo de limpieza de tráfico una respuesta de limpieza de tráfico, en donde la respuesta de limpieza de tráfico indica permiso para la limpieza del tráfico.

7. Un sistema de protección en un sistema en la nube, en donde el sistema en la nube comprende un nodo de protección y múltiples máquinas virtuales, los flujos de datos que se transmiten entre las máquinas virtuales pasan a través del nodo de protección, y el sistema de protección comprende:

un nodo (610) de protección en un sistema en la nube, configurado para recoger estadísticas sobre el tráfico de datos de entrada en una máquina virtual dentro de un tiempo fijado con antelación; si las estadísticas muestran que le tráfico de datos de entrada en la máquina virtual dentro del tiempo fijado con antelación excede un umbral fijado con antelación, determinar que el tráfico de datos de entrada en la máquina virtual es anormal; extraer los flujos de datos a ser introducidos en la máquina virtual si se detecta que el tráfico de datos de entrada en la máquina virtual es anormal, y enviarle los flujos de datos extraídos a un equipo de limpieza de tráfico para su limpieza; recibir los flujos de datos limpios devueltos por el equipo de limpieza de tráfico; e introducir los flujos de datos limpios en la máquina virtual; y

un equipo (620) de limpieza de tráfico, configurado para limpiar los flujos de datos procedentes del nodo de protección en el sistema en la nube y se van a introducir en la máquina virtual, y enviarle los flujos de datos limpios al nodo de protección en el sistema en la nube.

8. El sistema de protección de acuerdo con la reivindicación 7, en donde:

el nodo de protección en el sistema en la nube comprende un nodo de gestión de máquinas virtuales en el sistema en la nube.

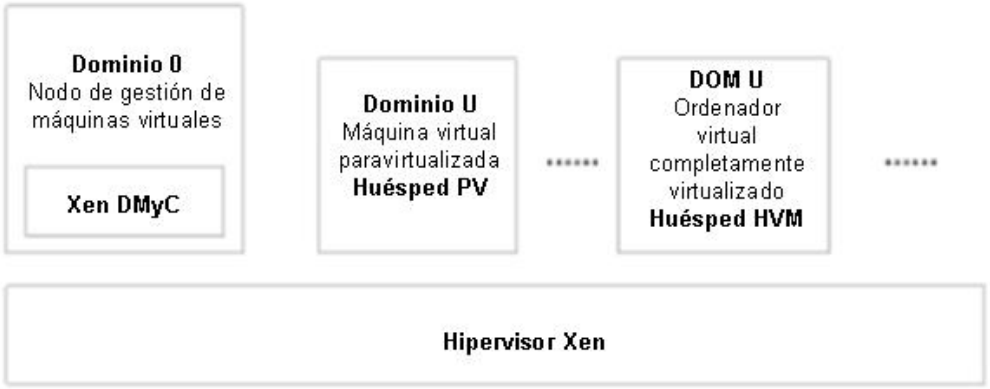
Dominio 0
Nodo de gestión de máquinas virtuales
Xen DMyC
Dominio U
Máquina virtual paravirtualizada
Huésped PV
.....
DOM U
Ordenador virtual completamente virtualizado
Huésped HVM
.....
Hipervisor Xen

FIG. 1-a

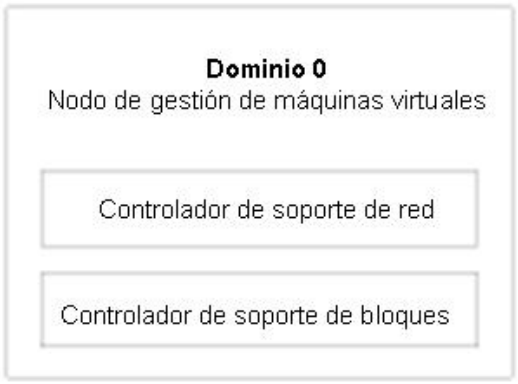
Dominio 0
Nodo de gestión de máquinas virtuales
Controlador de soporte de red
Controlador de soporte de bloques

FIG. 1-b

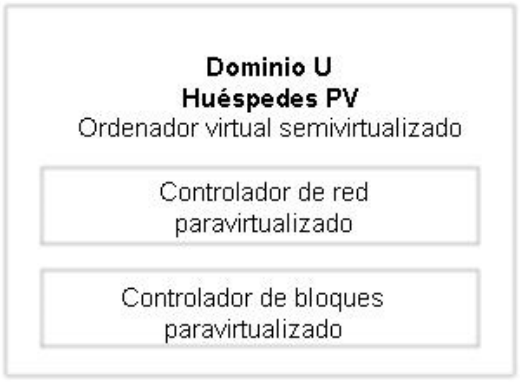
Dominio U
Huéspedes PV
Ordenador virtual semivirtualizado
Controlador de red paravirtualizado
Controlador de bloques paravirtualizado

FIG. 1-c

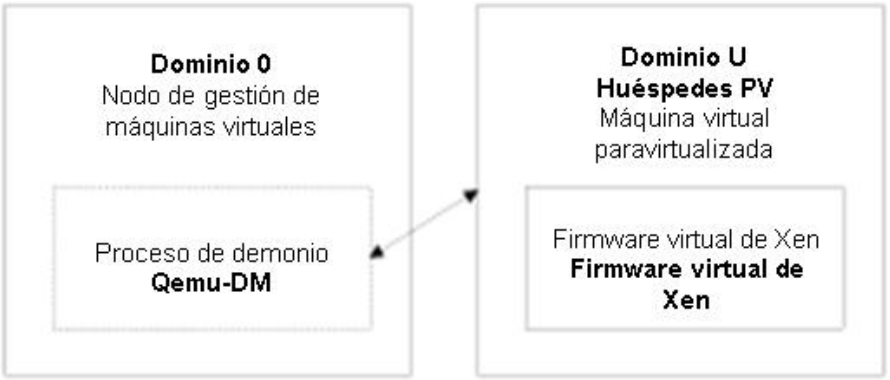
Dominio 0
Nodo de gestión de máquinas virtuales
Proceso de demonio
Qemu-DM
Dominio U
Huéspedes PV
Máquina virtual paravirtualizada
Firmware virtual de Xen
Firmware virtual de Xen

FIG. 1-d

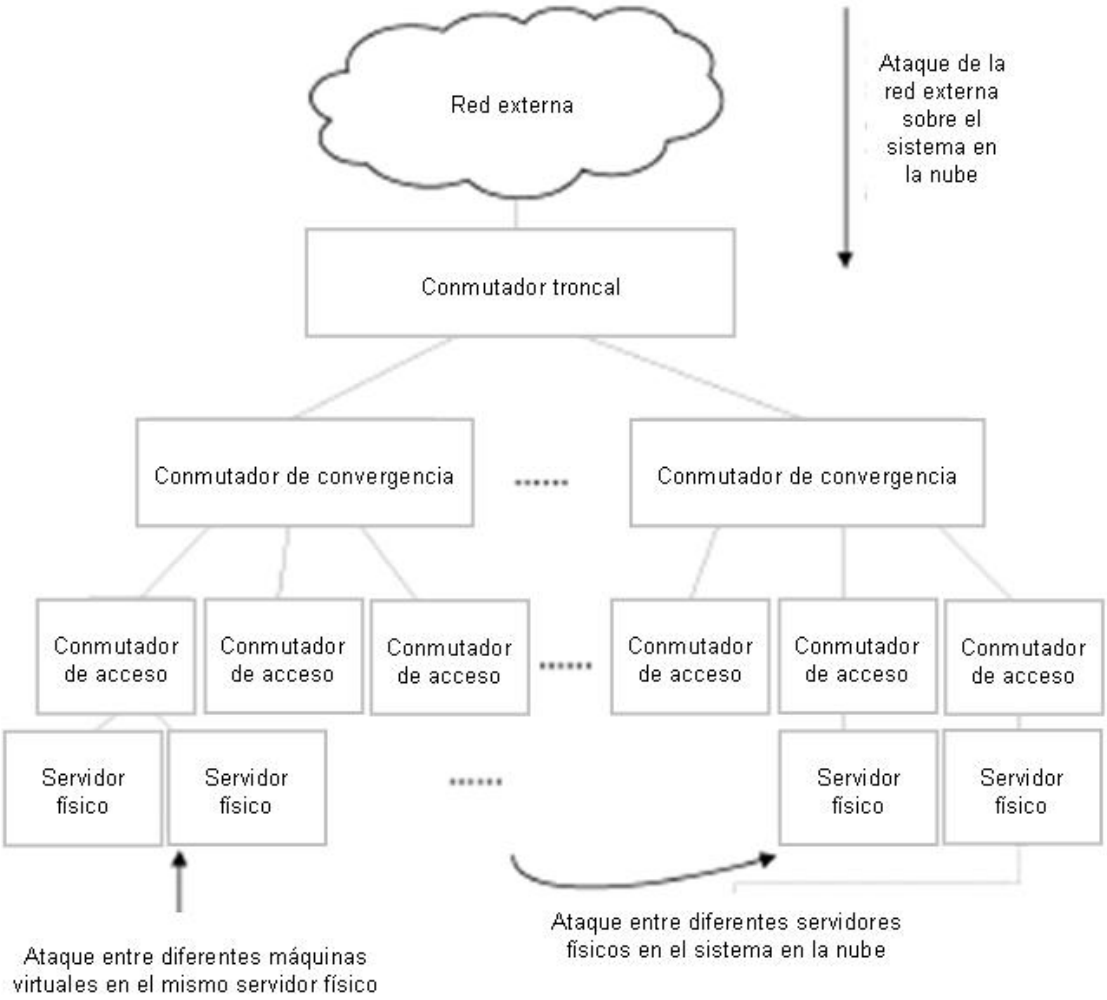
Red externa
Ataque de la red externa sobre el sistema en la nube
Conmutador troncal
Conmutador de convergencia
.....
Conmutador de convergencia
Conmutador de acceso
Conmutador de acceso
Conmutador de acceso
.....
Conmutador de acceso
Conmutador de acceso
Conmutador de acceso
Servidor físico
Servidor físico
.....
Servidor físico
Servidor físico
Ataque entre diferentes máquinas virtuales en el mismo servidor físico
Ataque entre diferentes servidores físicos en el sistema en la nube

FIG. 2

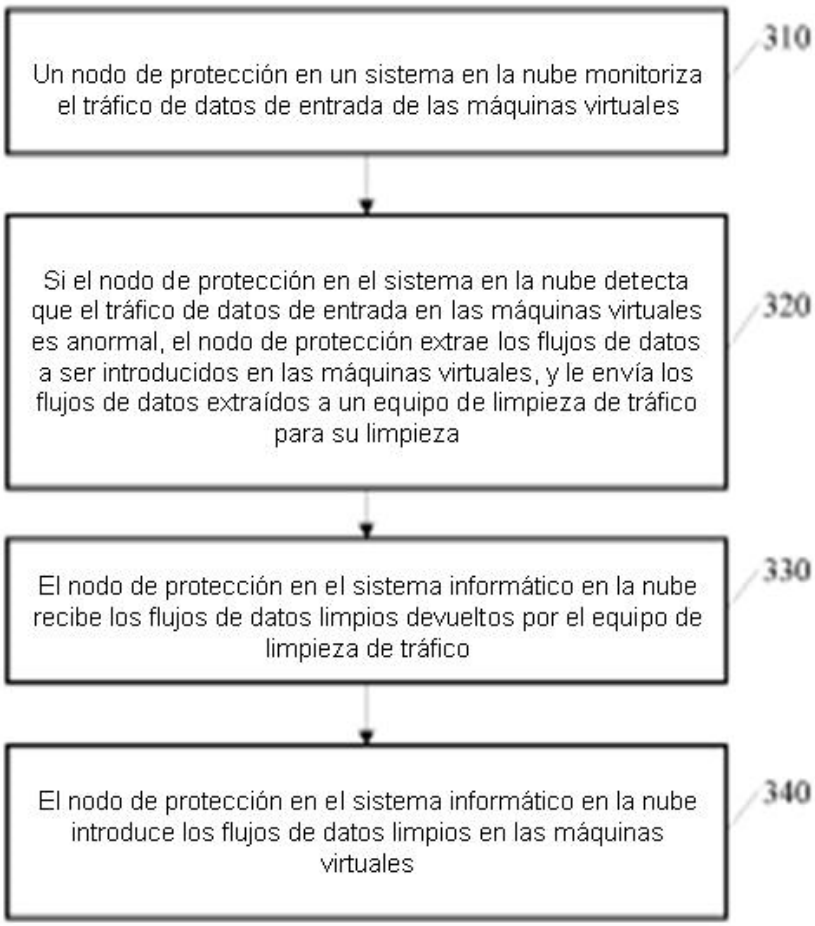
Un nodo de protección en un sistema en la nube monitoriza el tráfico de datos de entrada de las máquinas virtuales
310
Si el nodo de protección en el sistema en la nube detecta que el tráfico de datos de entrada en las máquinas virtuales es anormal, el nodo de protección extrae los flujos de datos a ser introducidos en las máquinas virtuales, y le envía los flujos de datos extraídos a un equipo de limpieza de tráfico para su limpieza
320
El nodo de protección en el sistema informático en la nube recibe los flujos de datos limpios devueltos por el equipo de limpieza de tráfico
330
El nodo de protección en el sistema informático en la nube introduce los flujos de datos limpios en las máquinas virtuales
340

FIG. 3

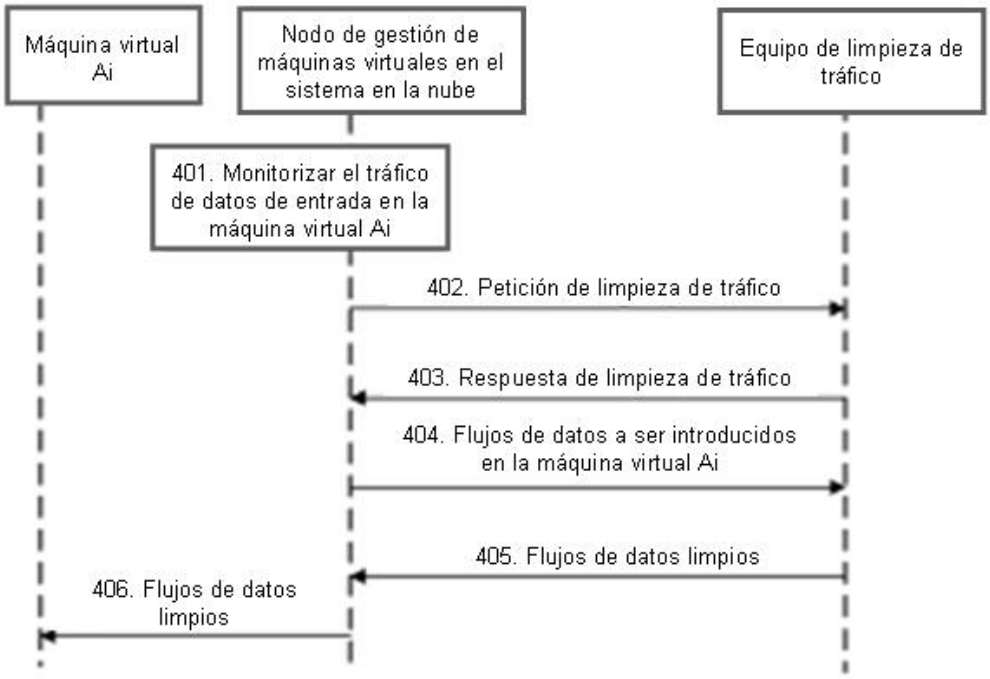
Máquina virtual Ai
Nodo de gestión de máquinas virtuales en el sistema en la nube
Equipo de limpieza de tráfico
401. Monitorizar el tráfico de datos de entrada en la máquina virtual Ai
402. Petición de limpieza de tráfico
403. Respuesta de limpieza de tráfico
404. Flujos de datos a ser introducidos en la máquina virtual Ai
405. Flujos de datos limpios
406. Flujos de datos limpios

FIG. 4

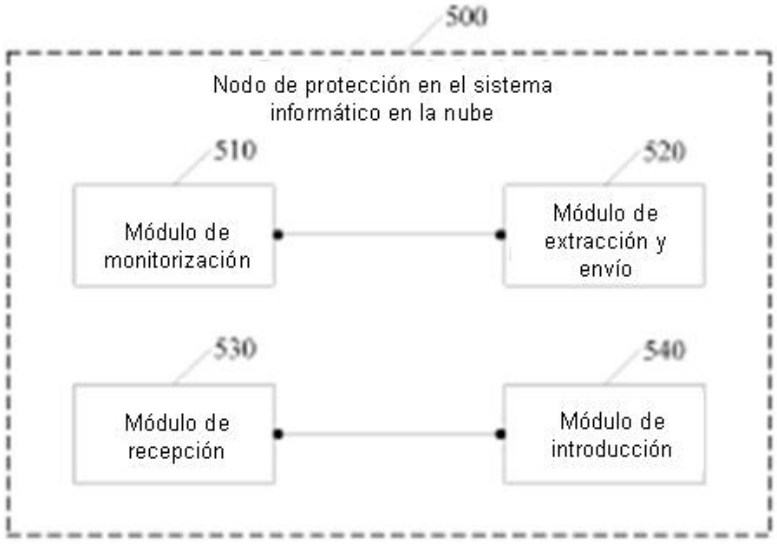
500
Nodo de protección en el sistema informático en la nube
510
Módulo de monitorización
520
Módulo de extracción y envío
530
Módulo de recepción
540
Módulo de introducción

FIG. 5-a

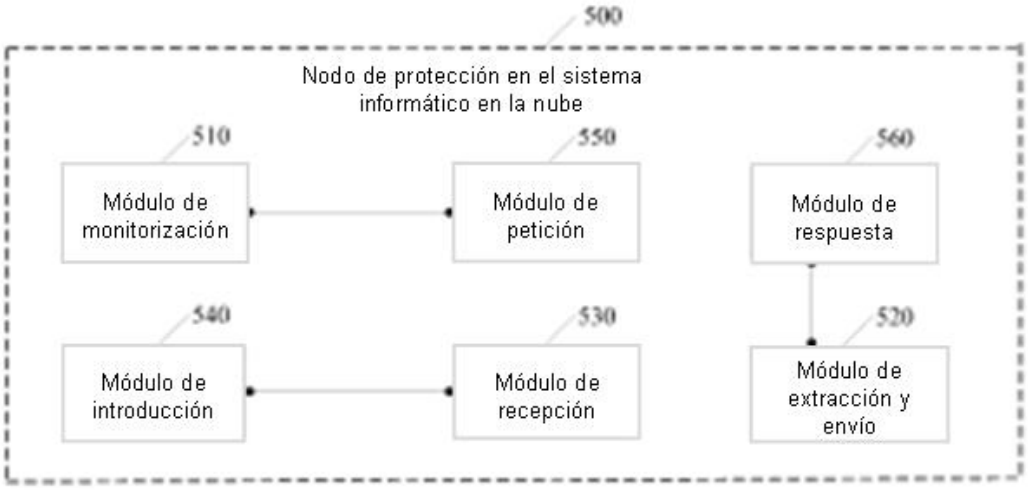
500
Nodo de protección en el sistema informático en la nube
510
Módulo de monitorización
550
Módulo de petición
560
Módulo de respuesta
540
Módulo de introducción
530
Módulo de recepción
520
Módulo de extracción y envío

FIG. 5-b


610
Nodo de protección en el sistema informático en la nube
620
Equipo de limpieza de tráfico

FIG. 6