(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 143**

(51) Int. CI.:
H04L 29/06 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08253837 .2**
(96) Fecha de presentación: **28.11.2008**
(97) Número de publicación de la solicitud: **2073496**
(97) Fecha de publicación de la solicitud: **24.06.2009**

(54) Título: **MARCO DE DISTRIBUCIÓN DE CLAVE SIMÉTRICA PARA INTERNET.**

(30) Prioridad:
14.12.2007 US 957184

(45) Fecha de publicación de la mención BOPI:
09.03.2012

(45) Fecha de la publicación del folleto de la patente:
09.03.2012

(73) Titular/es:
INTEL CORPORATION
2200 MISSION COLLEGE BOULEVARD
SANTA CLARA, CA 95052, US

(72) Inventor/es:
Kolar Sunder, Divya Naidu;
Dewan, Prashant y
Long, Men

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Marco de distribución de clave simétrica para Internet

Campo de la invención

La invención se refiere a la distribución constante y dinámica de claves simétricas desde un servidor de distribución de claves dedicado a clientes a través de Internet.

Antecedentes de la invención

El World Wide Web es fundamentalmente una aplicación cliente/servidor que se ejecuta a través de Internet. Las amenazas a la seguridad en Internet han aumentado exponencialmente en los últimos años. Una forma de clasificar las amenazas de seguridad diferentes en cuanto a la ubicación de la amenaza: servidor web, navegador web del cliente, y el tráfico entre el navegador web del cliente y el servidor. Teniendo en cuenta el tráfico entre el cliente y el servidor, que es fácil de implementar “Fuerza de tarea de ingeniería de Internet” (IETF), “Seguridad de protocolo de Internet” (IPSec) y TLS (“Seguridad de capa de transporte”), protocolos de seguridad basados en red, que dependen de la negociación de las claves de la sesión entre clientes y servidores utilizando criptografía de clave asimétrica cara (por ejemplo, Diffie-Hellman). Los servidores tienen que seguir la pista de decenas de miles de claves simétricas transitorias negociadas en función de cada sesión. El resultado es que las memorias que se vende por las asociaciones de seguridad para realizar las operaciones criptográficas para estos protocolos en hardware se convierten en prohibitivamente caras debido a la cantidad de estado que debe ser mantenido (por no hablar de los costes de la negociación de claves).

Tecnología relacionada se divulga en la publicación de la solicitud de patente US 2006/0047944 A1 de Roger Kilian-Kehr, indicándose las características de la misma en el preámbulo de cada reivindicación independiente. Este documento divulga técnicas que permiten un acceso al sistema informático de destino a los datos del usuario sólo después de la verificación de la fiabilidad del sistema informático de destino. El acceso se concede por una tercera parte de confianza que proporciona al sistema de destino una clave de descifrado en el establecimiento exitoso de la confiabilidad. Un módulo de plataforma segura (TPM) en el sistema de destino puede proporcionar el TTP con indicadores que reflejan la fiabilidad del sistema de destino. Protocolos conocidos "Alianza de plataforma informática segura" (TCPA) se utilizan para comunicarse entre el destino y el TPM.

Breve descripción de los dibujos

La presente invención se ilustra a modo de ejemplo y no está limitada por los dibujos, en los que referencias similares indican elementos similares, y en los que:

La figura 1 describe un dispositivo y un sistema para la distribución de clave simétrica a través de Internet.

La figura 2 es un diagrama de flujo de una realización de un proceso para distribuir información de las claves usando un servidor de distribución de claves.

Descripción detallada de la invención

Se describen realizaciones de un procedimiento, dispositivo y sistema de distribución de claves simétricas desde un servidor a los clientes a través de Internet. En la siguiente descripción, se indican numerosos detalles específicos. Sin embargo, se entiende que las realizaciones se pueden practicar sin estos detalles específicos. En otros casos, elementos, especificaciones y protocolos bien conocidos no han sido descritos en detalle con el fin de evitar el oscurecimiento de la presente invención.

La figura 1 describe un dispositivo y un sistema de distribución de claves simétricas a través de Internet. En muchas realizaciones, un cliente 100 está conectado a un dominio 102 a través de Internet 104. Internet es una serie en todo el mundo de las redes de ordenadores de acceso público interconectados que transmiten datos a través de protocolos tal como el protocolo de Internet (IP) estándar. Más específicamente, Internet es una "red de redes" que consiste en millones de pequeñas redes domésticas, académicas, empresariales y gubernamentales que, en conjunto, llevan información y servicios diversos. Físicamente, Internet incluye redes troncales por cable, ópticas e inalámbricas que comprenden el medio sobre el cual se transmite la información.

En diferentes formas de realización, el cliente puede ser un ordenador de sobremesa, un ordenador portátil, un dispositivo móvil inalámbrico, un teléfono celular, un decodificador para un televisor o cualquier otro tipo de dispositivo informático que tiene la capacidad de conectarse a Internet. La conexión del cliente a Internet puede ser a través de mecanismos tales como enrutadores, conmutadores, puntos de acceso, entre otros dispositivos que se conectan dispositivos individuales a Internet.

En diferentes realizaciones, el dominio puede ser un dominio para una red de una empresa, una institución científica, una universidad, una oficina del gobierno, una persona individual, entre otros. El dominio consiste en uno o más

servidores de sistemas informáticos que llevan a cabo una serie de funciones que permiten que la información pase entre los ordenadores y los usuarios en el dominio e Internet. Cada dominio tiene un nombre de dominio que se asigna a una dirección IP específica.

La figura 1 ilustra un ejemplo de una serie de servidores que realizan funciones vitales dentro del dominio. En diferentes realizaciones, estos servidores pueden ser máquinas separadas físicamente o pueden ser aplicaciones que se ejecutan en una sola máquina (por ejemplo, en distintas particiones de la máquina).

El cliente puede solicitar el acceso al dominio 102 para servicios. En muchas realizaciones, un servidor de aplicaciones 106 situado dentro del dominio proporciona uno o más de estos servicios que el cliente 100 desea (por ejemplo, servicio de almacenamiento de información, servicio de recuperación de noticias, servicio de correo electrónico, etc.).

En muchas realizaciones, el dominio 102 tiene un cortafuegos 108. El cortafuegos 108 es una forma de seguridad que trata de evitar que los usuarios y los programas malintencionados entren en el dominio de Internet 104. El cortafuegos 108 puede ser un servidor independiente (mostrado) o puede ser parte de uno de los otros servidores en la figura 1 (no mostrado).

El dominio también incluye un servidor DHCP (protocolo de configuración de huésped dinámico) 110. Suponiendo que el cliente 100 está configurado con DHCP, cuando el cliente 100 se conecta al dominio 102, el programa del cliente DHCP en el cliente 100 envía una consulta de difusión solicitando la información necesaria desde el servidor DHCP 110. El servidor DHCP 110 gestiona un conjunto de direcciones IP e información sobre los parámetros de configuración del cliente, tales como el nombre de dominio, la puerta de enlace predeterminada, entre otros. Además, el servidor DHCP 110 tiene información sobre la presencia y la dirección de un servidor DNS (sistema de nombres de dominio) 112 ubicado en el dominio 102. Tras la recepción de una solicitud válida desde el cliente 100, el servidor DHCP 110 asignará al cliente 100 una dirección IP y otros parámetros.

El cliente 100, ahora configurado con una dirección IP recibida desde el servidor DHCP 110 y la dirección del servidor DNS 112, puede ahora interactuar con el servidor DNS 112. El servidor DNS 112 proporciona direcciones IP de servidores y otros dispositivos dentro en el dominio 102.

Volviendo al servidor de aplicaciones 106, uno o más procesadores 114 están presentes en el servidor de aplicaciones 106. En realizaciones diferentes, cada uno de estos procesadores puede ser de uno o múltiples núcleos. Por lo tanto, en algunas realizaciones, el servidor de aplicaciones es un multiprocesador, servidor de múltiples núcleos y en otras realizaciones, el servidor de aplicaciones es de un solo procesador, servidor de un solo núcleo, y en otras realizaciones, el servidor de aplicaciones es un derivado de una combinación de los sistemas descritos anteriormente de procesador simple/múltiple, núcleo simple/múltiple. En otras realizaciones, puede haber más de un servidor de aplicaciones presente para servicios adicionales o el mismo servicio puede ser distribuido entre varios servidores de aplicaciones para equilibrar la carga del cliente. Muchas de las configuraciones descritas anteriormente de procesador y servidor no se muestran en la figura 1, ya que un solo procesador en un solo servidor proporciona una realización adecuada para describir la situación cliente/servidor.

Además, el servidor de aplicaciones 106 también incluye una memoria del sistema 116 para almacenar instancias actuales de uno o más sistemas operativos, tal como el sistema operativo (OS) 118. En operaciones normales, el procesador 114 en el servidor de aplicaciones 106 puede atender una serie de peticiones de los clientes a través de Internet 104, tal como un cliente 100. Después de pasar por los procedimientos de encaminamiento con el servidor DHCP 110 y el servidor DNS 112, el cliente normalmente interactúa con el servidor de aplicaciones 106 para tener acceso a los servicios del servidor de aplicaciones.

Aunque, en muchas realizaciones, el servidor de aplicaciones 106 puede tener una o más políticas de salud que requieren que cualquier cliente interactúe. Por ejemplo, puede haber un mínimo nivel requerido de salud que un cliente debe superar antes de que se conceda el acceso a interactuar con el servidor de aplicaciones 106. Estos niveles de salud pueden ser predeterminados o determinarse de forma dinámica en función del entorno. Si el nivel de salud no se cumple por un cliente, un controlador de interfaz de red (NIC) 120 puede rechazar paquetes de ese cliente. El NIC 120 es una interfaz de hardware que gestiona y permite que el servidor de aplicaciones 106 acceda a la red informática interna dentro del dominio.

Para determinar con seguridad la salud del cliente, en muchas realizaciones, un dispositivo de tecnología de gestión activa (AMT) de Intel® 122 u otro dispositivo de medición de seguridad independiente que funciona de forma similar a la AMT está presente en el cliente 100. En algunas realizaciones, la AMT 122 puede medir la salud del sistema del cliente. Esta medida puede incluir información tal como el software instalado en el cliente, el sistema operativo instalado en el cliente, la versión de software antivirus instalado en el cliente, y cuan reciente y la cantidad de ataques se ha gestionado el sistema del cliente, entre otros elementos de información . Lógica dentro de la AMT 122 puede obtener esta información, o la lógica de cualquier otra parte del cliente 100 puede recopilar la información de la salud y la AMT 122 puede verificar la autenticidad de la información de salud. Una vez que esta información de salud se reúne,

la AMT 122 puede firmar la información de salud con un certificado digital de seguridad. El cliente 100 entonces puede enviar la información de salud segura a través de Internet 104 al dominio 102.

En muchas realizaciones, una vez que el cliente 100 ha recibido inicialmente la dirección IP del servidor de aplicaciones 106, el cliente 100 solicita los requisitos de la política de salud del servidor de aplicaciones 106 para ver qué requisitos son necesarios para interactuar con el servidor de aplicaciones 106. En muchas realizaciones, un programa de resolución que se ejecuta en el cliente 100 busca la política de salud del cliente que se requiere en el servidor de aplicaciones 106. Esta solicitud podrá ser gestionada directamente por el NIC 120. El NIC 120 puede almacenar información de la política de salud asociada con el servidor de aplicaciones 106 que reside dentro y puede dar servicio a las peticiones de política de salud de cualquier cliente, de manera que ninguna carga de solicitud inicial requiere la interacción directa con el procesador 114, la memoria 116, o el sistema operativo 118.

Además de los requisitos de la política de salud para los clientes, el programa de resolución, después de realizar una política de salud del cliente busca en el servidor de aplicaciones, también puede notificar al cliente de solicitudes que el dominio 102 incluye un servidor de distribución de claves (KDS) 124 o múltiples KDS. Esta información se obtendría mediante el programa de resolución durante la búsqueda. El KDS 124 es capaz de validar la información de salud recibida de los clientes. Una vez validado, el KDS 124 puede proporcionar al cliente una clave de sesión específica del cliente para una interacción segura con el servidor de aplicaciones 106. Se presume que el KDS 124 en el dominio 102 es de confianza para el servidor de aplicaciones 106.

El NIC 120 en el servidor de aplicaciones puede ser proporcionado por el KDS 124 con la clave maestra para la generación de claves de sesión. Por ejemplo, una vez que el KDS 124 ha autenticado la salud del cliente, el KDS puede generar una clave maestra para una sesión entre el cliente 100 y el servidor de aplicaciones 106. El KDS 124 envía una clave de sesión, que se genera a partir de la información de identificación del cliente y la clave maestra para el cliente 100.

En algunas realizaciones, la clave de sesión se envía al cliente usando el protocolo SSL (capa de ranuras segura). En otras realizaciones, la clave de sesión se envía al cliente usando el protocolo TLS (seguridad de capa de transporte). Los protocolos TLS y SSL permiten las comunicaciones privadas a través de una red de una forma diseñada para prevenir el espionaje, la manipulación y la falsificación de mensajes. Estos protocolos proporcionan autenticación de punto final y la privacidad de las comunicaciones a través de Internet utilizando criptografía.

El KDS 124 también envía la clave maestra al NIC 120 en el servidor de aplicaciones 106. Utilizando la clave de sesión recibida del KDS 124, el cliente puede establecer ahora una conexión cifrada y autentificada con el servidor de aplicaciones. El cliente puede enviar paquetes cifrados al servidor de aplicaciones 106 usando un formato de paquete IPSec (seguridad de protocolo de Internet). El paquete de formato del encabezado del paquete IPSec incluye un campo de índice de parámetros de seguridad (SPI) que tiene la información de identificación del cliente.

Una vez que el NIC 120 recibe un paquete IPSec desde el cliente 100, la lógica en el NIC 120 verifica la identidad del cliente dentro del SPI, y, utilizando la clave maestra recibida del KDS 124, genera el lado del servidor de la clave simétrica usando una función clave tal como:

Clave de sesión = f (clave maesta, SPI del cliente)

Una vez que versión del NIC 120 de la clave de la sesión se genera, el NIC 120 puede descifrar el paquete del cliente 100 y envía los paquetes desencriptados a la pila de software de red en el servidor de aplicaciones 106 de manera que el procesador 114 y OS 118 puedan usar el paquete.

Si el descifrado de los paquetes no tiene éxito, el NIC 120 puede descartar el paquete. Esto eliminará cualquier sobrecarga realizada por el procesador 114, ya que el procesador 114 nunca vería el paquete.

Por lo tanto, mediante la utilización del sistema y de un dispositivo KDS descrito anteriormente, KDS puede realizar la mayoría, si no todas, las operaciones de distribución de claves criptográficas, por lo tanto, eliminando este importante volumen de trabajo del servidor de aplicaciones 106. Además, el procesador 114 y el OS 118 que residen en el servidor de aplicaciones 106 también se eliminan del trabajo de descifrado porque el NIC 120 es independientemente capaz de descifrar los paquetes entrantes y enviar los paquetes descifrados junto a la pila de red que reside en el software del servidor de aplicaciones 106.

En muchas realizaciones, hay múltiples KDSs distribuidos en el dominio 102. Los múltiples KDSs pueden proporcionar beneficios tales como el equilibrio de la carga de la distribución de claves a muchos clientes, así como proporcionar una mayor seguridad mediante la distribución de la funcionalidad del KDS, de manera que un ataque a cualquier servidor no sería capaz de burlar el sistema de distribución de claves. Cualquier algoritmo de equilibrio general de carga de servidores distribuidos puede ser utilizado para equilibrar la carga entre los múltiples KDSs. Por ejemplo, el programa de resolución en el cliente 100, después de realizar una búsqueda de DNS para el KDS mediante la interacción con el servidor DNS 112, puede aplicar un algoritmo de equilibrio de carga a la dirección IP devuelta del

KDS. Esto puede enviar la solicitud de clave del cliente a cualquiera de los muchos KDSs presentes en el dominio.

Además, en muchas realizaciones, el NIC 120 podrá informar al KDS 124, cuando se producen una o más situaciones anormales con los paquetes entrantes de los clientes. El KDS 124 puede tomar las medidas adecuadas respecto a uno o más clientes cuando haya sido informado de este comportamiento anormal del NIC 120. Por ejemplo, el KDS 124 puede guardar una lista de revocación de claves y/o clientes. Por lo tanto, si el NIC 120 informa al KDS 124 cuando ve los paquetes que contienen el mismo ID de cliente, pero en diferentes direcciones IP, entonces el KDS 124 puede poner la clave asociada con el ID de cliente en la lista de revocación y distribuir una nueva clave para el cliente. Si el NIC 120 informa al KDS 124 que esta nueva clave vuelve a ser utilizada por varios clientes, el cliente que solicitó la clave puede ser puesto en la lista de revocación para denegar de forma permanente a ese cliente más comunicación con cualquier servidor de la red.

En muchas realizaciones, la información sobre la salud del KDS 124 que se recibe desde un cliente también podría estar superpuesta con otra información del cliente, incluyendo las capacidades del cliente y los roles potenciales (es decir, información de postura). El KDS 124 puede utilizar esta información adicional para decidir qué servidores dentro del dominio del cliente 102 se le permitirá comunicarse con ellos. Por lo tanto, el KDS 124 puede enviar un conjunto de claves utilizadas para comunicarse con este conjunto determinado de servidores.

La figura 2 es un diagrama de flujo de una realización de un proceso para distribuir información de la clave mediante un servidor de distribución de claves. El proceso se puede realizar por hardware, software, o una combinación de ambos. El proceso comienza mediante el procesamiento lógico en una máquina del cliente que solicita un servidor DHCP en un dominio para proporcionar la dirección IP del servidor DNS en el dominio y también una dirección IP para el cliente (bloque de procesamiento 200). Entonces la lógica de procesamiento en el servidor DHCP contesta con la dirección IP del servidor DNS y el cliente (bloque de procesamiento 202).

El proceso continúa con la lógica de procesamiento en el cliente que solicita al servidor DNS buscar la dirección IP de un servidor de aplicaciones en el dominio (bloque de procesamiento 204). Entonces la lógica de procesamiento responde al servidor DNS con la dirección IP del servidor de aplicaciones (bloque de procesamiento 206). El procesamiento lógico dentro de un programa de resolución de clientes entonces, utilizando la dirección IP del servidor de aplicaciones, pregunta al servidor de aplicaciones para buscar la validación de la salud y la política de autentificación del servidor de aplicaciones (bloque de procesamiento 208).

Los resultados de la búsqueda de la política de resolución de clientes en el servidor de aplicaciones se determinan entonces mediante la lógica de procesamiento (bloque de procesamiento 210). Si el servidor de aplicaciones no tiene una política presente, entonces la lógica de procesamiento en el cliente procede con una petición HTTP regular al servidor de aplicaciones (bloque de procesamiento 212).

De lo contrario, si la política de validación/acreditación de la salud está presente, entonces la lógica de procesamiento sabe que un servidor KDS está presente en el dominio. Por lo tanto, la lógica de procesamiento en el cliente solicita la dirección IP del servidor KDS del servidor DNS (bloque de procesamiento 214). A continuación, el servidor DNS responde al cliente con la dirección IP del servidor KDS (bloque de procesamiento 216). La lógica de procesamiento en el cliente luego mide la salud del cliente (bloque de procesamiento 218). La medición de la salud se puede hacer utilizando un dispositivo AMT u otro dispositivo utilizado para verificar que la máquina del cliente es saludable y no está comprometida. La lógica de procesamiento en el cliente a continuación proporciona la información de la salud y potencialmente otra información de la postura al servidor KDS (bloque de procesamiento 220).

La lógica de procesamiento en el servidor KDS a continuación realiza un procedimiento de validación de la información de la salud del cliente medida (bloque de procesamiento 222). Este procedimiento de validación puede ser cualquiera de una serie de políticas de requisitos de salud. Esto debe decidirse en una base servidor a servidor basada en el nivel de seguridad requerido para el acceso del cliente al servidor de aplicaciones en el dominio.

En este punto, la lógica de procesamiento ha determinado la salud del cliente (bloque de procesamiento 224). Si el cliente no se considera saludable por el servidor KDS, el servidor KDS no envía una clave de sesión al cliente (bloque de procesamiento 226). De lo contrario, si el cliente es considerado saludable por el servidor KDS, el servidor KDS envía una clave de sesión única (es decir, la clave de derivación) al cliente (bloque de procesamiento 228). Cuando el cliente recibe la clave, la lógica de procesamiento en el cliente continúa con una solicitud segura al servidor de aplicaciones utilizando la clave de sesión única (bloque de procesamiento 230). Finalmente, la lógica de procesamiento en el NIC del servidor de aplicaciones recibe la solicitud segura por parte del cliente y descifra el paquete con una clave de sesión derivada de la identificación del cliente y una llave maestra proporcionada desde el KDS (bloque de procesamiento 232). Una vez que el paquete se descifra, el paquete puede ser enviado a la pila de software de red para su posterior procesamiento en el servidor de aplicaciones y el proceso ha terminado.

De este modo, se describen realizaciones de un procedimiento, dispositivo y sistema de distribución de claves simétricas desde un servidor a clientes a través de Internet. Estas realizaciones se han descrito con referencia a

determinados ejemplos de realización de las mismas. Es evidente que las personas que tengan el beneficio de esta exposición que varias modificaciones y cambios se pueden hacer a estas realizaciones, sin apartarse del alcance de las realizaciones descritas en este documento. La memoria y los dibujos, en consecuencia, deben considerarse de forma ilustrativa y no un sentido restrictivo.

REIVINDICACIONES

1. Procedimiento, que comprende:

un servidor de distribución de claves que recibe información de la salud medida de un cliente;

el servidor validando la información de salud medida;

el servidor enviando una clave de sesión al cliente cuando la información de salud medida se valida, y

al recibir la clave de sesión, el cliente inicia una conexión cifrada y autentificada con un servidor de aplicaciones en el dominio;

caracterizado porque:

un controlador de interfaz de red en el servidor de aplicaciones recibe uno o más paquetes cifrados desde el cliente a través de la conexión autentificada;

el controlador de la interfaz de red descifra el uno o más paquetes cifrados con la clave de sesión;

el controlador de interfaz de red descarta el uno o más paquetes si el descifrado no tiene éxito; y

si la desencriptación tiene éxito, el servidor de aplicaciones proporciona uno o más paquetes descifrados.

2. Procedimiento según la reivindicación 1, en el que el servidor de distribución de claves es direccionable en un dominio de Internet.

3. Procedimiento según la reivindicación 2, que también comprende:

el cliente busca una política de cliente en el servidor de distribución de claves;

sobre la base de la política de distribución de claves del cliente del servidor, el cliente mide la información sobre la salud del cliente; y

el cliente firma la información de salud medida del cliente.

4. Procedimiento según la reivindicación 1, en el que uno o más paquetes cifrados son paquetes de seguridad de protocolo Internet (IPSec).

5. Dispositivo, que comprende:

una lógica del servidor de distribución de claves operable para

recibir información de la salud medida desde un cliente,

validar la información de salud medida, y

enviar una clave de sesión al cliente cuando la información de salud medida se valida;

caracterizado porque:

la lógica del servidor de aplicaciones incluye un controlador de interfaz de red, el controlador es operable para:

recibir un paquete desde el cliente, en el que el paquete se cifra usando la clave de sesión;

descifrar el paquete utilizando la clave de sesión; y

descartar el paquete si el descifrado no es exitoso;

y

la lógica del servidor de aplicaciones es operable para

proporcionar el paquete descifrado si la desencriptación tiene éxito.

6. Dispositivo según la reivindicación 5, en el que el dispositivo es direccionable en un dominio de Internet.

7. Dispositivo según la reivindicación 5, en el que el dispositivo es también operable para almacenar una política del cliente para indicar al cliente uno o más requisitos necesarios para interactuar con el dispositivo.

8. Sistema, que comprende:

un cliente;

un servidor de distribución de claves operable para

recibir información de salud medida del cliente,

validar la información de salud medida, y

enviar una clave de sesión al cliente cuando la información de salud medida se valida; y

un servidor de aplicaciones que comprende:

una memoria para almacenar un sistema operativo;

un procesador operable para ejecutar instrucciones del sistema operativo;

caracterizado porque el servidor de aplicaciones también comprende:

un controlador de interfaz de red operable para

recibir un paquete desde el cliente, en el que el paquete se cifra usando la clave de sesión,

descifrar el paquete utilizando la clave de sesión,

descartar el paquete cuando el descifrado no es correcto;

enviar el paquete desencriptado al sistema operativo para su uso por el procesador cuando la descripción es exitosa, y

en el que el procesador no realiza ninguna operación en el paquete cuando el controlador de interfaz de red descarta el paquete.

9. Sistema según la reivindicación 13, que también comprende un servidor de nombres de dominio operable para proporcionar la dirección del servidor de distribución de claves al cliente.

10. Sistema según la reivindicación 13, en el que el cliente comprende un componente de gestión de seguridad operable para medir la salud del dispositivo del cliente,

generar información de salud del cliente basada en la medición, y

firmar la información de salud medida del cliente.

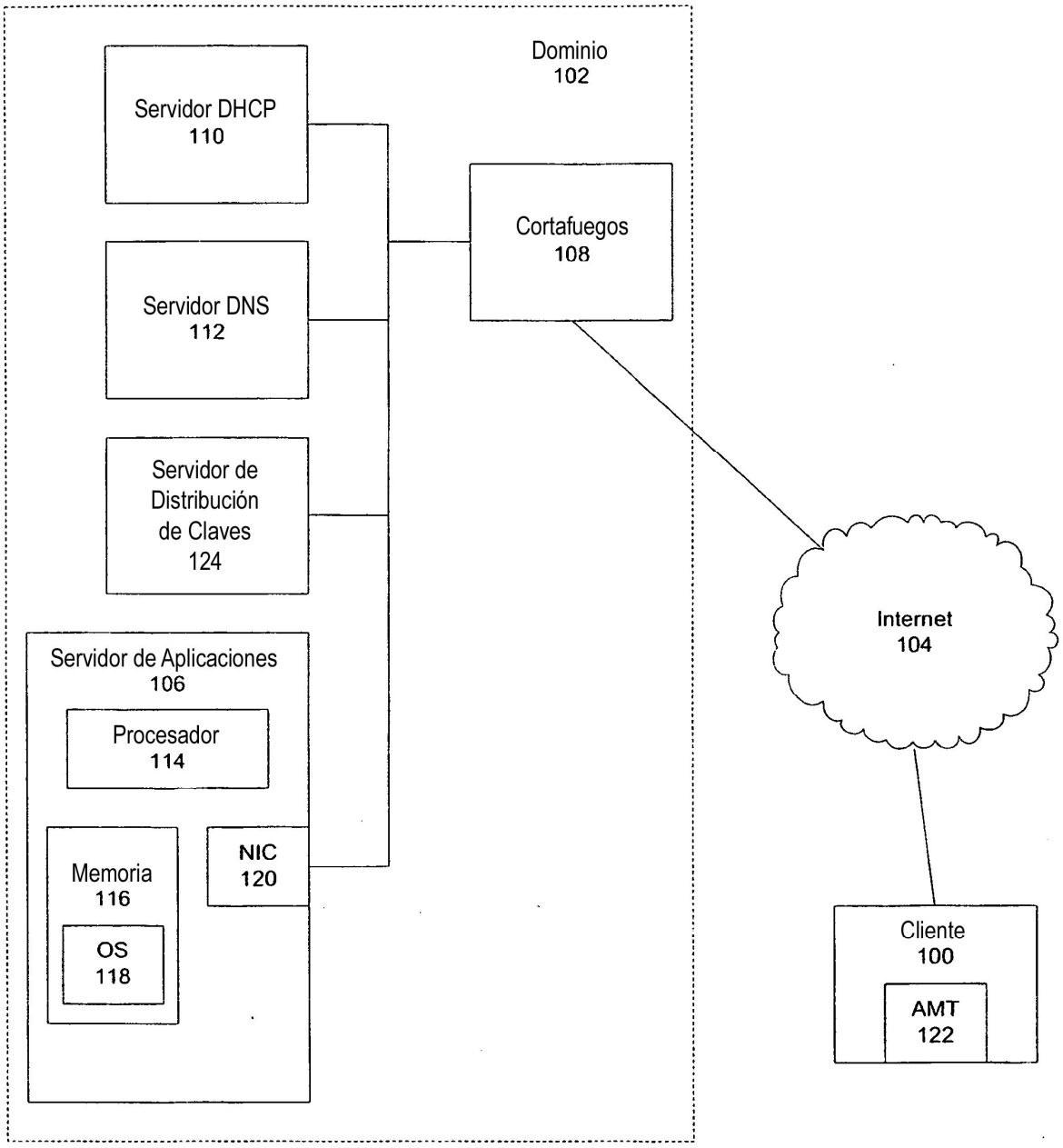
Dominio
102
Servidor DHCP
110
Servidor DNS
112
Servidor de
Distribución
de Claves
124
Cortafuegos
108
Internet
104
Servidor de Aplicaciones
106
Procesador
114
Memoria
116
OS
118
NIC
120
Cliente
100
AMT
122

FIG. 1

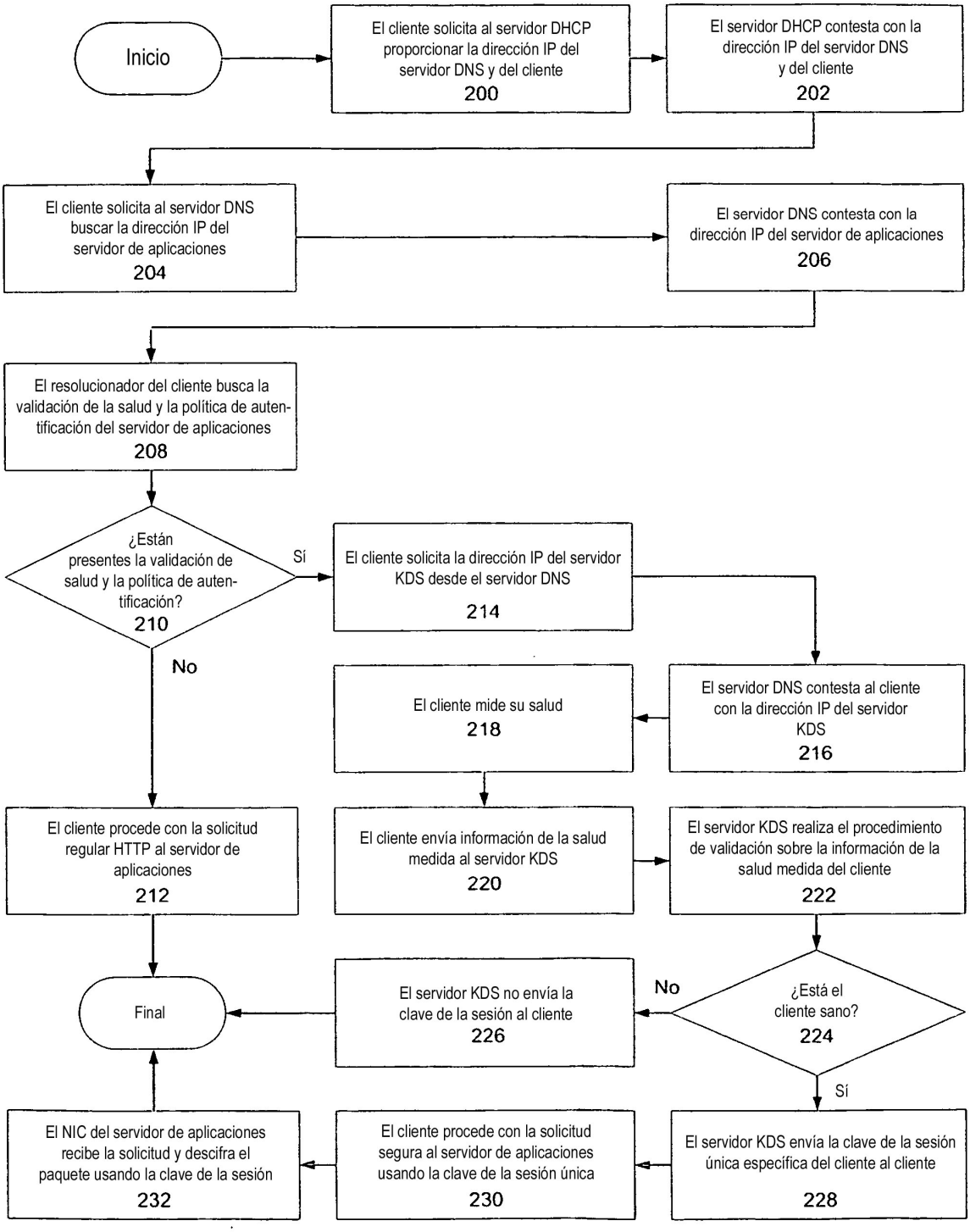
Inicio
El cliente solicita al servidor DHCP proporcionar la dirección IP del servidor DNS y del cliente
200
El servidor DHCP contesta con la dirección IP del servidor DNS y del cliente
202
El cliente solicita al servidor DNS buscar la dirección IP del servidor de aplicaciones
204
El servidor DNS contesta con la dirección IP del servidor de aplicaciones
206
El resolucionador del cliente busca la validación de la salud y la política de autenticación del servidor de aplicaciones
208
¿Están presentes la validación de salud y la política de autenticación?
210
Sí
No
El cliente solicita la dirección IP del servidor KDS desde el servidor DNS
214
El servidor DNS contesta al cliente con la dirección IP del servidor KDS
216
El cliente mide su salud
218
El cliente procede con la solicitud regular HTTP al servidor de aplicaciones
212
El cliente envía información de la salud medida al servidor KDS
220
El servidor KDS realiza el procedimiento de validación sobre la información de la salud medida del cliente
222
Final
El servidor KDS no envía la clave de la sesión al cliente
226
No
¿Está el cliente sano?
224
Sí
El NIC del servidor de aplicaciones recibe la solicitud y descifra el paquete usando la clave de la sesión
232
El cliente procede con la solicitud segura al servidor de aplicaciones usando la clave de la sesión única
230
El servidor KDS envía la clave de la sesión única específica del cliente al cliente
228

FIG. 2