(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 457**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.02.2013 PCT/IL2013/000017**

(87) Fecha y número de publicación internacional: **22.08.2013 WO13121410**

(96) Fecha de presentación y número de la solicitud europea: **13.02.2013 E 13749686 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2815554**

(54) Título: **Procedimiento de acceso inverso para proteger aplicaciones de entrada y otras**

(30) Prioridad:

19.02.2012 IL 21818512

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.04.2017

(73) Titular/es:

MIZHAR, AMIR (100.0%)
7/7 Shvat Street
7173093 Modiin, IL

(72) Inventor/es:

MIZHAR, AMIR

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de acceso inverso para proteger aplicaciones de entrada y otras

Campo técnico

Lo que sigue es una invención para proteger datos almacenados electrónicamente, al ordenador en el que residen los datos y a las comunicaciones del ordenador con su red informática.

Técnica antecedente

Es un hecho muy conocido que los ordenadores de la red interna de una organización (también denominada red de área local o LAN) que proporcionan servicios a usuarios ajenos a la organización son muy propensos a ataques procedentes de piratas informáticos externos y de código malicioso. Debido a este riesgo, es una práctica común proteger la LAN poniendo los ordenadores orientados hacia el exterior en una subred segregada y blindar con ello al resto de la red en caso de ataque. Esta subred es denominada comúnmente DMZ (zona desmilitarizada). Cualquier ordenador que ejecute programas que proporcionen servicios a usuarios ajenos a la red interna de la organización puede ser puesto en la DMZ. Los tipos más comunes de ordenadores son los servidores de páginas electrónicas, los servidores de correo electrónico, los servidores de FTP y los servidores de VoIP.

Dado que la DMZ es una subred que contiene los servicios externos de la organización hacia una red mayor en la que no se confía (habitualmente Internet), piratas informáticos potenciales y código malicioso pueden lograr el acceso a la DMZ, pero raramente logran el acceso a la LAN. Los ordenadores de la DMZ tienen conectividad limitada a los ordenadores de la LAN y suelen estar separados por un cortafuegos que controla el tráfico entre los ordenadores de la DMZ y los ordenadores de la LAN. Se puede interpretar que la DMZ es una capa adicional de seguridad para la LAN.

Las organizaciones que tienen portales de Internet que permiten las comunicaciones con el público general a través de Internet son vulnerables a una infiltración desde el exterior. Por lo tanto, muchas de estas organizaciones establecen una DMZ para proteger sus datos sensibles y reducir la capacidad de los piratas informáticos de infiltrar la LAN. Las maneras y los procedimientos con los que funciona la DMZ son conocidos por cualquier experto en la técnica y, por lo tanto, no hay ninguna necesidad de describirlos aquí con detalle adicional.

Establecer una DMZ requiere la duplicación de datos relevantes y programas informáticos para que puedan residir tanto en los ordenadores de la DMZ como en los ordenadores de la LAN.

Esta duplicación de datos y programas informáticos tiene varios inconvenientes. Puede resultar costoso comprar licencias adicionales requeridas para instalar múltiples instancias del mismo programa informático tanto en la LAN como en la DMZ. Dar soporte y gestionar programas informáticos y datos en la LAN y en la DMZ puede resultar costoso y difícil. Además, dado que la DMZ se comunica con sistemas externos, los datos de la DMZ son vulnerables a ataques de piratas informáticos y a código externo malicioso.

La siguiente invención se propone superar estas desventajas y proporcionar un sistema eficiente para proteger los datos de la LAN.

El documento US 4824798 es técnica antecedente adicional.

Descripción de los dibujos

La intención de los dibujos adjuntos a la solicitud no es limitar el alcance de la invención ni su aplicación. Los dibujos están pensados únicamente para ilustrar la invención y constituyen únicamente una de sus muchas implementaciones posibles.

La **Figura 1** describe el sistema, que incluye la LAN (30), que incluye el servicio (33), el servidor LAN (31) y el controlador LAN (32); la DMZ (20), que incluye el servidor DMZ (21), el servicio (22) del colectivo de pilas DMZ; y la WAN (10); y las conexiones entre estos componentes.

La invención

Según se ha descrito anteriormente, hay una gran necesidad de un sistema informático que permita que los usuarios se comuniquen con la LAN y que, a la vez, proteja a la LAN de amenazas externas. La siguiente invención proporciona una solución eficiente de los problemas que se mencionan anteriormente.

La presente invención proporciona un sistema para proteger los datos y los ordenadores centrales que residen en la LAN y, a la vez, permite a los usuarios comunicarse con la **LAN** de forma segura.

En aras de la claridad y para simplificar la explicación del sistema, se usan los términos siguientes: **WAN:** red (10) de área amplia; **DMZ:** zona desmilitarizada (20); **LAN:** red (30) de área local; **servidor LAN:** servidor (31) que se

ejecuta en la LAN; **servidor DMZ:** servidor (21) que se ejecuta en la DMZ; **servicio del colectivo de pilas DMZ:** almacena y gestiona las solicitudes (22) del cliente en la DMZ; **solicitud de cliente:** protocolos HTTP/HTTPS (navegador de páginas electrónicas)/SSH/SFTP/FIT/FTPS/RDP/SMTP/TLS y cualquier otro basado en TCP/IP; **información de conexión del cliente**: dirección IP/número de puerto del servicio relevante de destino dentro de la LAN; **controlador LAN:** un controlador (32) que se ejecuta en la LAN que gestiona la información de conexión del cliente; **enlace de conexión:** establecimiento de comunicación entre dos interfaces de conexión TCP/IP; **servicio**: servicios HTTP/HTTPS (servidor de páginas electrónicas)/SSH/SFTP/FTP/FTPS/RDP/SMTP/TLS y cualquier otro basado en TCP/IP.

El objetivo de la presente invención es proporcionar una conexión segura entre los servidores de la LAN y los clientes de la WAN.

La **Figura 1** describe los principales componentes del sistema. La LAN (30) incluye el servicio (33), el servidor LAN (31) y el controlador LAN (32); la DMZ (20) incluye el servidor DMZ (21), el servicio (22) del colectivo de pilas DMZ; y la WAN (10), que, por su naturaleza, incluye los clientes y el mundo “exterior”. Además, la Fig. 1 describe las conexiones entre los componentes del sistema. Las conexiones entre los componentes del sistema serán descritas mientras se describe el flujo del sistema. El flujo de conexiones del sistema es como sigue:

Primera etapa: La solicitud del cliente (del cliente (11)) llega al servidor DMZ (21). Segunda etapa: El servidor DMZ (21) almacena la solicitud del cliente en el servicio (22) del colectivo de pilas DMZ. Tercera etapa: El controlador LAN (32) establece una conexión (41) saliente basada en TCP con el servicio (22) del colectivo de pilas DMZ. Uno de los aspectos innovadores del sistema es que el controlador LAN (32) verifica de forma constante y/o en un conjunto predefinido de momentos, las solicitudes de cliente almacenadas en el servicio (22) del colectivo de pilas DMZ. Cuarta etapa: El servicio (22) del colectivo de pilas DMZ pasa entonces la información de conexión del cliente al servidor LAN (31) por medio del controlador LAN (32).

Quinta etapa: El servidor LAN (31) genera entonces dos conexiones TCP/IP: una conexión es con el servicio (33), que es el servicio de destino, en función de la información de conexión del cliente. La segunda conexión es una conexión saliente (42) al servidor DMZ (21). Además, el servidor LAN (31) crea un enlace de conexión en el servidor LAN entre el servicio (33) y la conexión saliente (42). Sexta etapa: El servidor DMZ (21) crea a continuación un enlace de conexión en el servidor DMZ entre la solicitud entrante de cliente (que está almacenada en el servicio del colectivo de pilas DMZ (22)) y la conexión saliente (42) procedente del servidor LAN (31), y con eso completa la ruta de la solicitud del cliente.

Una vez que el enlace de conexión en el servidor DMZ enlaza la solicitud del cliente y la conexión saliente (42) procedente del servidor LAN, la solicitud del cliente es finalmente difundida a través del servidor DMZ y el servidor LAN por el sistema, y a continuación los datos de la solicitud del cliente son difundidos desde el servicio (33) al cliente (11).

Según la presente invención descrita en lo que antecede, no se requiere ninguna gestión administrativa en el servidor LAN (31) para establecer o mantener comunicaciones después de que sea instalado y configurado inicialmente en la LAN (30) y en la DMZ (20). El controlador LAN (32) consulta permanente o periódicamente al servicio del colectivo de pilas DMZ (22) en pos de solicitudes entrantes de cliente. El servidor DMZ (20) aceptará todas las solicitudes de cliente y las encaminará al servidor LAN (31) sin cambiar los datos que las solicitudes de cliente contienen. Por ejemplo, si una solicitud de cliente usa el protocolo de conexión HTTPS, entonces por el sistema se transmitirá el protocolo de conexión HTTPS, como con cualesquiera otras protocolos comunes, tales como SSH/SFTP/FTP/FTPS/RDP/SMTP/TLS o cualesquiera otros protocolos basados en TCP/IP.

REIVINDICACIONES

1. Un sistema que proporciona una conexión segura entre servidores de la LAN y clientes de la WAN que comprende: LAN y DMZ; en el que la LAN incluye el servicio, el servidor LAN y el controlador LAN; en el que la DMZ incluye el servidor DMZ y el servicio del colectivo de pilas DMZ; en el que, cuando una solicitud de cliente llega al servidor DMZ, este almacena la solicitud del cliente en el servicio del colectivo de pilas DMZ; en el que el controlador LAN establece una conexión saliente basada en TCP con el servicio del colectivo de pilas DMZ; en el que el servicio del colectivo de pilas DMZ pasa a continuación la información de conexión del cliente al servidor LAN por medio del controlador LAN; en el que el servidor LAN genera entonces dos conexiones TCP/IP: una conexión es con el servicio y la segunda es con una conexión saliente al servidor DMZ y que crea un enlace de conexión en el servidor LAN entre el servicio y la conexión saliente; en el que el servidor DMZ crea a continuación un enlace de conexión en el servidor DMZ entre la solicitud entrante de cliente y la conexión saliente procedente del servidor LAN;
completando con ello la ruta de la solicitud del cliente; y por lo que, una vez que el enlace de conexión en el servidor DMZ enlaza la solicitud del cliente y la conexión saliente procedente del servidor LAN, la solicitud del cliente es finalmente difundida a través del servidor DMZ y el servidor LAN por el sistema, y a continuación los datos de la solicitud del cliente son difundidos desde el servicio al cliente.

2. El sistema según la reivindicación 1, en el que el controlador LAN verifica de forma constante y/o en un conjunto predefinido de momentos, las solicitudes de cliente almacenadas en el servicio del colectivo de pilas DMZ.

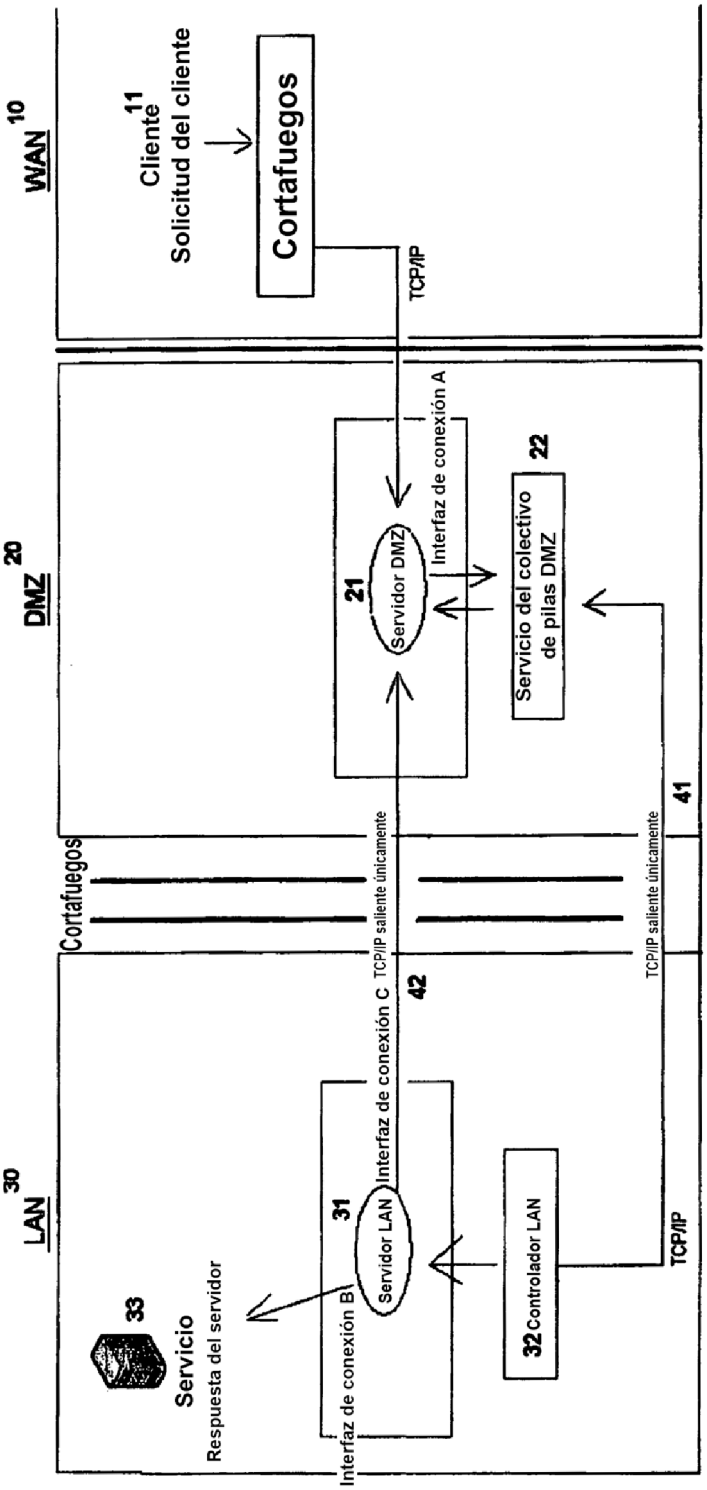
WAN 10
Cliente 11
Solicitud del cliente
Cortafuegos
TCP/IP
DMZ 20
Interfaz de conexión A
21
Servidor DMZ
22
Servicio del colectivo de pilas DMZ
Cortafuegos
TCP/IP saliente únicamente
41
TCP/IP saliente únicamente
42
Interfaz de conexión C
LAN 30
31
Servidor LAN
32 Controlador LAN
TCP/IP
33
Servicio
Respuesta del servidor
Interfaz de conexión B

Fig. 1