(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 August 2013 (22.08.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/121410 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/22* (2006.01)

(21) International Application Number:
PCT/IL2013/000017

(22) International Filing Date:
13 February 2013 (13.02.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
218185 19 February 2012 (19.02.2012) IL

(72) Inventor; and
(71) Applicant : **MIZHAR, Amir** [IL/IL]; 7/7 Shvat Street, 7173093 Modiin (IL).

(74) Agent: **DAHAN, Meir**; P.O. Box 174, Mitspe Adi 1794000 (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

WO 2013/121410 A1

(54) Title: REVERES ACCESS METHOD FOR SECURING FRONT-END APPLICATIONS AND OTHERS

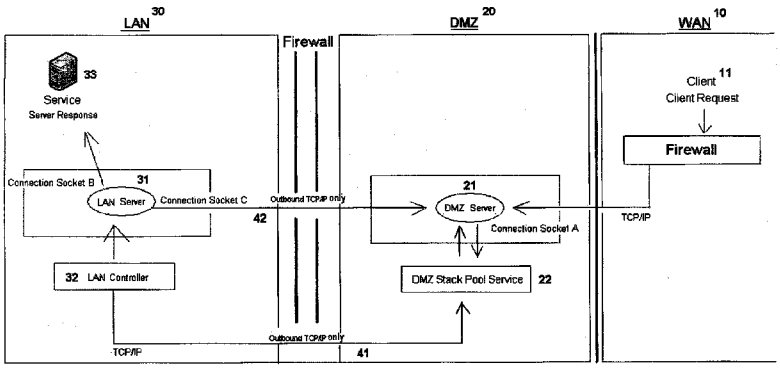

Fig 1

(57) Abstract: A System that provides a secured connection between servers on the LAN and clients on the WAN comprises the LAN (which includes LAN Service, LAN Server and LAN Controller) and the DMZ (which includes DMZ Server and DMZ Stack Pool Service). Wherein the Client Request reaches the DMZ Server it stores it in the DMZ Stack Pool Service and the LAN Controller establishes outbound TCP based connection to the DMZ Stack Pool Service that passes the Client Connection Information to the LAN Server via the LAN Controller. Then the LAN Server then generates a connection between the Service and the DMZ Server.

Reveres Access Method for Securing Front-End Applications and Others

Description

TECHNICAL FIELD

The following is an invention for securing electronically stored data, the computer on which the data resides on and the communications of the computer with its computer network.

BACKGROUND ART

It is a well-known fact that the computers in an organization's internal network (also known as the local area network or LAN) which provide services to users outside of the organization are highly prone to attacks from external hackers and malicious code. Due to this risk, it is a common practice to protect the LAN by placing external-facing computers in a segregated sub-network and thereby shield the rest of the network in case of an attack. This sub-network is commonly known as the DMZ (or De-Militarized Zone). Any computer running programs that provide services to users outside of the organization's internal network can be placed on the DMZ. The most common type of computers are web servers, email servers, FTP servers and VoIP servers.

Since the DMZ is a sub-network that contains the organization's external services to a larger untrusted network (usually the Internet), potential hackers and malicious code may gain access to the DMZ, but rarely do they gain access to the LAN. The computers on the DMZ have limited connectivity to the computers on the LAN and are usually separated by a firewall that controls the traffic between the DMZ computers and the LAN computers. The DMZ can be seen as an additional layer of security to the LAN.

Organizations that have Internet portals which enable communications with the general public via the Internet are vulnerable to infiltration from the outside. Therefore, many of these organizations establish a DMZ to protect their sensitive data and to reduce the ability of hackers to infiltrate the LAN. The ways and methods under which the DMZ works is known to any expert in the field, and therefore there is no need to describe them here in further detail.

Establishing a DMZ requires the duplication of relevant data and computer programs so they can reside on both the DMZ computers and on the LAN computers.

This duplication of data and computer programs has several drawbacks. It can be costly to purchase additional licenses required to install multiple instances of the same computer program on both the LAN and on the DMZ. Supporting and managing duplicate computer programs and data on the LAN and on the DMZ can be costly and difficult. Furthermore, since the DMZ interfaces with the external systems, the data on the DMZ is vulnerable to hacking attacks and external malicious code.

The following invention aims to overcome these disadvantages and to provide an efficient system for protecting the data on the LAN.

DESCRIPTION OF THE DRAWINGS

The intention of the drawings attached to the application is not to limit the scope of the invention and its application. The drawings are intended only to illustrate the invention and they constitute only one of its many possible implementations.

Figure 1 describes the System that includes the LAN (30) which includes the Service (33), the LAN Server (31) and the LAN Controller (32); The DMZ (20) which includes the DMZ Server (21), the DMZ Stack Pool Service (22); and the WAN (10); and the connections between these components.

THE INVENTION

As described above, there is a strong need for a computer system that enables users to communicate with the LAN and in the same time protects the LAN from external threats. The following invention provides an efficient solution for the issues that are mentioned above.

The present invention provides a System for securing the data and the hosts that reside in the LAN and in the same time enable users to communicate with the LAN in a secured way.

For the sake of clarity and for simplifying the explanation of the System, the following terms are used: **WAN**: Wide Area Network (10); **DMZ**: De-Militarized Zone (20); **LAN**: Local Area Network (30); **LAN Server**: Server running in the LAN (31); **DMZ Server**: Server running in the DMZ (21); **DMZ Stack Pool Service**: Stores and handles Client's Requests (22) in the DMZ; **Client Request**: HTTP/HTTPS (Web browser)/ SSH/SFTP/FTP/FTPS/RDP/SMTP/TLS, and any other TCP/IP based protocols; **Client Connection Information**: IP-address/ Port number of the relevant destination service inside the LAN; **LAN Controller**: a controller running in the LAN that manages the Client Connection Information (32); **Connection Binder**: Handshake between two TCP/IP sockets; **Service**: HTTP/HTTPS (Web Server)/ SSH/SFTP/FTP/FTPS/RDP/SMTP/TLS, and any other TCP/IP based services.

The objective of this invention is to provide a secured connection between servers in the LAN and the clients in the WAN.

Figure 1 describes the main components of the System. The LAN (30) includes the Service (33), the LAN Server (31) and the LAN Controller (32); The DMZ (20) includes the DMZ Server (21), the DMZ Stack Pool Service (22); and the WAN (10) that by its nature includes the clients and the 'outside' world. In addition, Fig. 1 describes the connections between the System components.

The connections between the System components will be described while describing the System flow. The connection flow of the System is as follow:

First step: The Client Request (of the client (11)) reaches the DMZ Server (21). Second step: The DMZ Server (21) stores the Client Request in the DMZ Stack Pool Service (22). Third step: The LAN Controller (32) establishes outbound TCP based connection (41) to the DMZ Stack Pool Service (22). One of the innovative aspects of the System is that the LAN Controller (32) constantly, and/or on a predefined set of time basis, checks for Client Requests stored in the DMZ Stack Pool Service (22). Forth step: The DMZ Stack Pool Service (22) then passes the Client Connection Information, to the LAN Server (31) via the LAN Controller (32).

The Fifth step: The LAN Server (31) then generates two TCP/IP connections: One connection is to the Service (33), which is the destination service, based on the Client Connection Information. The second connection is an outbound connection (42) to the DMZ Server (21). In addition the LAN Server (31) creates a Connection Binder in the LAN Server between the Service (33) and the outbound connection (42). The Sixth step: The DMZ Server (21) then creates a Connection Binder in the DMZ Server between the incoming Client Request (that is stored in the DMZ Stack Pool Service (22)) and the outbound connection (42) arriving from the LAN Server (31), and by that completes the route of the Client Request.

Once the Connection Binder, in the DMZ Server, binds the Client Request and the outbound connection (42) arriving from the LAN Server, the Client Request is then streamed through the DMZ Server and the LAN Server over the System, and then the client request data streams from the Service (33) to the Client (11).

In accordance with this invention as described above, no administrative management is required in the LAN Server (31) to establish or maintain communications after it is initially installed and configured on the LAN (30) and on the DMZ (20). The LAN Controller (32) permanently or periodically queries the DMZ Stack Pool Service (22) for incoming Client Requests. The DMZ Server (20) will accept all Client Requests and route them to the LAN-Server (31), without changing the data that the Client Requests contains. For example, if a Client Request uses the HTTPS connection protocol, then the HTTPS connection protocol will be transmitted over the System, as with any other common protocols such as SSH/SFTP/FTP/FTPS/RDP/SMTP/TLS/ or any other TCP/IP based protocols.

Claims

What is claimed is:

1. A System that provides a secured connection between servers on the LAN and clients on the WAN comprising: LAN and DMZ; wherein the LAN includes Service, LAN Server and the LAN Controller; wherein the DMZ includes DMZ Server and DMZ Stack Pool Service; wherein when a Client Request reaches the DMZ Server it stores the Client Request in the DMZ Stack Pool Service; wherein the LAN Controller establishes outbound TCP based connection to the DMZ Stack Pool Service; wherein the DMZ Stack Pool Service then passes the Client Connection Information, to the LAN Server via the LAN Controller; wherein the LAN Server then generates two TCP/IP connections: One connection is to the Service and the second is an outbound connection to the DMZ Server and creating a Connection Binder in the LAN Server between the Service and the outbound connection; wherein the DMZ Server then creates a Connection Binder in the DMZ Server between the incoming Client Request and the outbound connection arriving from the LAN Server;

Whereby by completing the route of the Client Request; and whereby once the Connection Binder, in the DMZ Server, binds the Client Request and the outbound connection arriving from the LAN Server, the Client Request is finally streamed through the DMZ Server and the LAN Server over the System, and then the client request data streams from the Service to the Client.

2. The System in accordance with claim 1 wherein the LAN Controller constantly, and/or on a predefined set of time basis, checks for Client Requests stored in the DMZ Stack Pool Service.

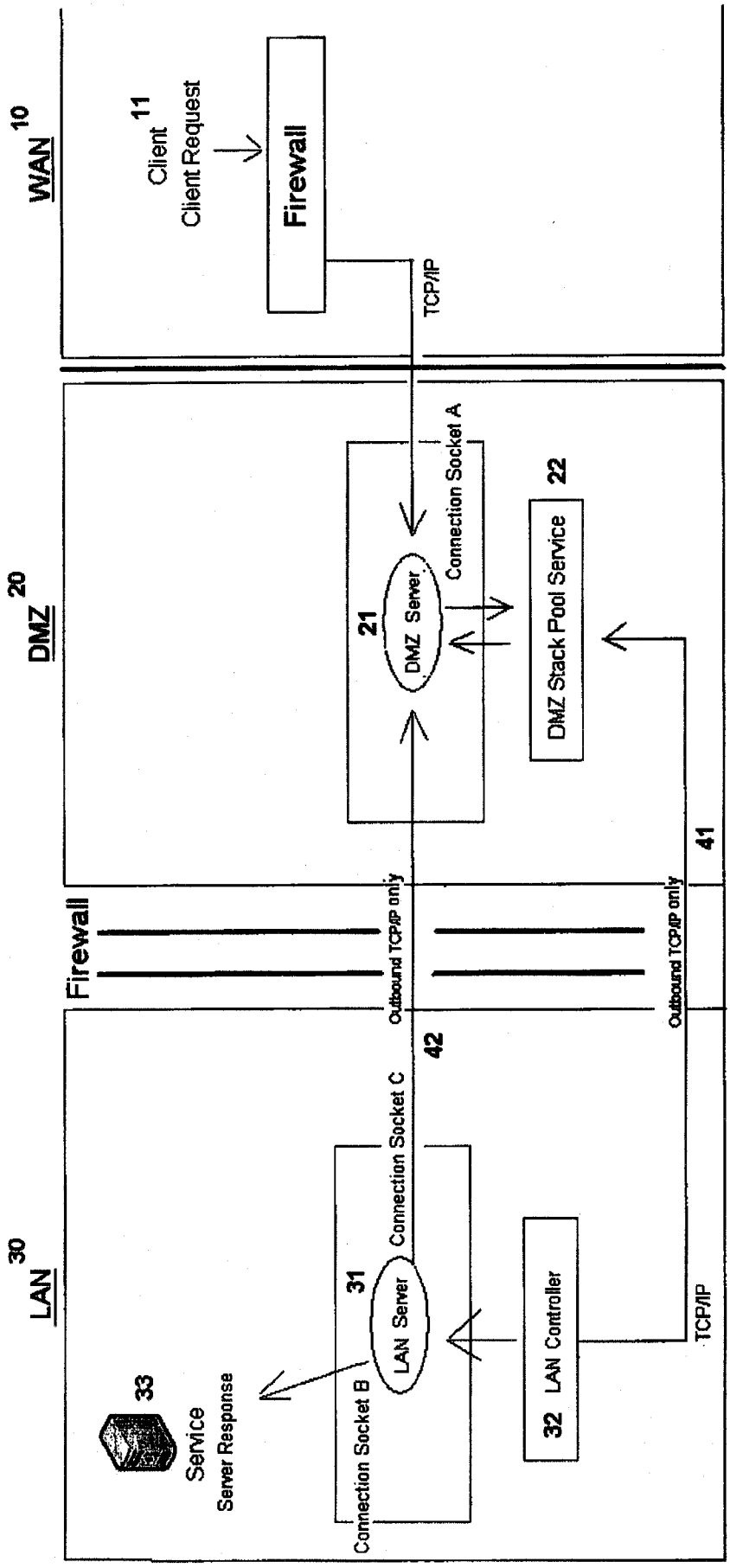
WAN 10
Client 11
Client Request
Firewall
TCP/IP
DMZ 20
Connection Socket A
21
DMZ Server
22
DMZ Stack Pool Service
Firewall
Outbound TCP/IP only
41
42
Outbound TCP/IP only
LAN 30
Connection Socket C
31
LAN Server
32 LAN Controller
TCP/IP
33
Service
Server Response
Connection Socket B

Fig 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2013/000017

A. CLASSIFICATION OF SUBJECT MATTER

IPC (2013.01) H04L 29/06, H04L 12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC (2013.01) H04L 12/22, H04L 29/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases consulted: PATENTSCOPE, Esp@cenet, Google Patents

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2031817 A1 Software Ag 04 Mar 2009 (2009/03/04) Entire document	1,2
A	US 7181493 B2 Unisys Corporation 20 Feb 2007 (2007/02/20) Entire document	1,2
A	US 6470386 B1 Worldcom, Inc. 22 Oct 2002 (2002/10/22) Entire document	1,2

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 Jul 2013	03 Jul 2013

Name and mailing address of the ISA:	Authorized officer
Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	AKERMAN Albert Telephone No. 972-2-5651754

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2013/000017

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
EP 2031817 A1	04 Mar 2009	CN 101420455 A	29 Apr 2009
		EP 2031817 A1	04 Mar 2009
		EP 2031817 B1	07 Nov 2012
		US 2009064307 A1	05 Mar 2009
		US 8181238 B2	15 May 2012
US 7181493 B2	20 Feb 2007	AU 2004308406 A1	14 Jul 2005
		CA 2550982 A1	14 Jul 2005
		EP 1704489 A2	27 Sep 2006
		EP 1704489 A4	28 Feb 2007
		US 2005216555 A1	29 Sep 2005
		US 7181493 B2	20 Feb 2007
		WO 2005062888 A2	14 Jul 2005
		WO 2005062888 A3	22 Sep 2005
		WO 2005062888 A9	12 Oct 2006
US 6470386 B1	22 Oct 2002	AU 752622 B2	26 Sep 2002
		AU 753269 B2	10 Oct 2002
		AU 755614 B2	19 Dec 2002
		AU 1062499 A	12 Apr 1999
		AU 3792997 A	21 Jan 1998
		AU 9582798 A	12 Apr 1999
		AU 9582998 A	12 Apr 1999
		AU 9583198 A	12 Apr 1999
		AU 9583298 A	12 Apr 1999
		AU 9583398 A	12 Apr 1999
		AU 9583598 A	12 Apr 1999
		AU 9583698 A	12 Apr 1999
		AU 9584098 A	12 Apr 1999
		AU 9666398 A	12 Apr 1999
		AU 9667198 A	12 Apr 1999

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2013/000017

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		AU 9667298 A	12 Apr 1999
		AU 9667598 A	12 Apr 1999
		AU 9667698 A	12 Apr 1999
		AU 9667898 A	12 Apr 1999
		AU 9667998 A	12 Apr 1999
		AU 9668098 A	12 Apr 1999
		AU 9668298 A	03 May 1999
		AU 9777098 A	12 Apr 1999
		AU 9777298 A	12 Apr 1999
		AU 9777398 A	12 Apr 1999
		BR 9814046 A	02 Jan 2002
		BR 9814049 A	20 Nov 2001
		BR 9814050 A	13 Nov 2001
		CA 2304543 A1	22 Apr 1999
		CA 2304554 A1	01 Apr 1999
		CA 2304619 A1	01 Apr 1999
		EP 1015970 A2	05 Jul 2000
		EP 1015970 A4	30 Jul 2003
		EP 1015986 A1	05 Jul 2000
		EP 1015986 A4	23 Jul 2003
		EP 1015995 A1	05 Jul 2000
		EP 1015995 A4	30 Jul 2003
		JP 2003522342 A	22 Jul 2003
		JP 2003525475 A	26 Aug 2003
		JP 2003526126 A	02 Sep 2003
		US 5610915 A	11 Mar 1997
		US 5825769 A	20 Oct 1998
		US 6032184 A	29 Feb 2000
		US 6115040 A	05 Sep 2000
		US 6141777 A	31 Oct 2000
		US 6377993 B1	23 Apr 2002

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 2001052013 A1	13 Dec 2001
		US 6381644 B2	30 Apr 2002
		US 6385644 B1	07 May 2002
		US 6470386 B1	22 Oct 2002
		US 6473407 B1	29 Oct 2002
		US 6490620 B1	03 Dec 2002
		US 6515968 B1	04 Feb 2003
		US 6574661 B1	03 Jun 2003
		US 6587836 B1	01 Jul 2003
		US 2003041263 A1	27 Feb 2003
		US 6598167 B2	22 Jul 2003
		US 6606708 B1	12 Aug 2003
		US 6611498 B1	26 Aug 2003
		US 6615258 B1	02 Sep 2003
		US 6631402 B1	07 Oct 2003
		US 6714979 B1	30 Mar 2004
		US 6745229 B1	01 Jun 2004
		US 6763376 B1	13 Jul 2004
		US 2002087383 A1	04 Jul 2002
		US 6859783 B2	22 Feb 2005
		US 2002054587 A1	09 May 2002
		US 6956845 B2	18 Oct 2005
		US 2004019808 A1	29 Jan 2004
		US 6968571 B2	22 Nov 2005
		US 7058600 B1	06 Jun 2006
		US 2003191970 A1	09 Oct 2003
		US 7114083 B2	26 Sep 2006
		US 7225249 B1	29 May 2007
		US 2006098583 A1	11 May 2006
		US 7236486 B2	26 Jun 2007
		US 2005172018 A1	04 Aug 2005

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 7447736 B2	04 Nov 2008
		US 2005210296 A1	22 Sep 2005
		US 7814533 B2	12 Oct 2010
		US 2005216421 A1	29 Sep 2005
		US 8073777 B2	06 Dec 2011
		US 2004193512 A1	30 Sep 2004
		US 2005114712 A1	26 May 2005
		US 2006129499 A1	15 Jun 2006
		US 2010024012 A1	28 Jan 2010
		US 2013111576 A1	02 May 2013
		WO 9800784 A1	08 Jan 1998
		WO 9915950 A1	01 Apr 1999
		WO 9915960 A2	01 Apr 1999
		WO 9915960 A3	20 May 1999
		WO 9915974 A1	01 Apr 1999
		WO 9915975 A1	01 Apr 1999
		WO 9915977 A1	01 Apr 1999
		WO 9915978 A1	01 Apr 1999
		WO 9915979 A1	01 Apr 1999
		WO 9915979 A9	14 Oct 1999
		WO 9915984 A1	01 Apr 1999
		WO 9915988 A2	01 Apr 1999
		WO 9915988 A3	28 Oct 1999
		WO 9915989 A1	01 Apr 1999
		WO 9915989 A9	26 Aug 1999
		WO 9915996 A2	01 Apr 1999
		WO 9915996 A3	20 May 1999
		WO 9916002 A1	01 Apr 1999
		WO 9916099 A2	01 Apr 1999
		WO 9916099 A3	20 May 1999
		WO 9916198 A1	01 Apr 1999

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2013/000017

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		WO 9916202 A2	01 Apr 1999
		WO 9916203 A2	01 Apr 1999
		WO 9916203 A3	07 Oct 1999
		WO 9916206 A1	01 Apr 1999
		WO 9916207 A1	01 Apr 1999
		WO 9916218 A1	01 Apr 1999
		WO 9916230 A1	01 Apr 1999
		WO 9919803 A1	22 Apr 1999