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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 January 2003 (09.01.2003)

PCT

(10) International Publication Number
WO 03/003666 A1

(51) International Patent Classification[7]: H04L 12/46

(21) International Application Number: PCT/SE01/01474

(22) International Filing Date: 27 June 2001 (27.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **HYGLO AB** [SE/SE]; Västberga Alle' 60, S-126 75 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BYSTRÖM, Leif** [SE/SE]; Tegelbruksvägen 37, S-126 34 Hägersten (SE).

(74) Agents: **SOHLMAN, Leif** et al.; Telia Reseach AB, Koncernpatent, S-123 86 Farsta (SE).

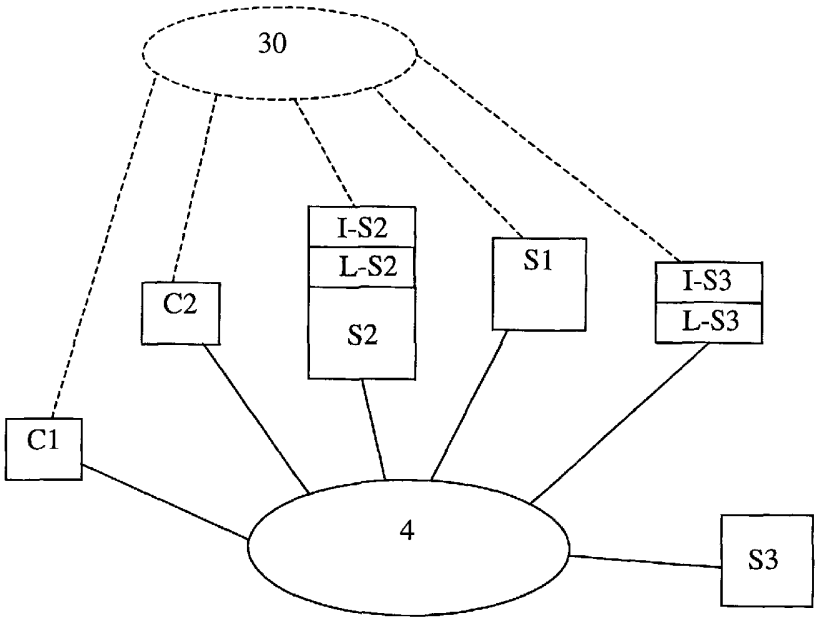
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PROVIDING SERVICES IN VIRTUAL PRIVATE NETWORKS



(57) Abstract: System for providing a service to a client (C1, C2) in a virtual network (30) residing on but being logically separated from a physical network (4), in which system a network service is located in a server (S2, S3). The system is characterised in that a logical representation (L-S2, L-S3) of the network service is provided, and connected to the virtual network by a virtual administrative interface (I-S2, I-S3). Preferably said logical representation includes a mapping to the network service, thereby representing a virtual service accessible to said client.

WO 03/003666 A1

SYSTEM AND METHOD FOR PROVIDING SERVICES IN VIRTUAL PRIVATE NETWORKS

Field if the invention

The invention relates in general to computer networks and more in particular to enabling mechanisms for delegation and distribution of centralised network server functions to the edge of computer networks. More specifically the invention relates to the problem of providing services to clients in virtual private networks.

Background

Most enterprises are located at multiple sites where each site has its own local area network (LAN). A site is defined as anything from a head-quarter, or an affiliation company site, to a single employee's remote office site. Some kind of communication infrastructure is then used to interconnect the different sites. The Internet evolution can roughly be categorised into two main areas:

a) Internet as the global communication infrastructure. Traditionally, companies used so called leased lines, provided by telephone companies to interconnect their sites. Separated firewall solutions were used for accessing the Internet. During the last years, companies are no longer using Internet only for external communication, more and more companies are trying out new network solutions that enables them to also use Internet for company-internal communication. Internet has become their site-to-site interconnecting medium.

b) Broadband Internet access. In parallel with the above, more and more broadband access solutions are rolled out by different network access providers. This enables anyone to upgrade their access to Internet from a traditional dial-up PSTN/ISDN (Public Switched Telephone Network/Integrated Services Digital Network) access solution to a broadband solution, e.g. ADSL (Asymmetric Digital Subscriber Line), Cable or Ethernet, with direct access to Internet. Apart from the obvious broadband benefits, the network access user is also able to always be connected to the Internet.

The common name for most of the network solutions that interconnects multiple sites over Internet is "virtual private networks" (VPN). VPNs can be implemented in numerous ways, this is well explained in e.g. the IETF by B. Gleeson et. al, "A Framework for IP Based Virtual private Networks", RFC 2764, February 2000. A VPN is a private network that is configured within a public network. For years, common carriers have built VPNs that appear as private national or international networks to the customer, but physically share backbone trunks with other customers. VPNs enjoy the security of a private network via access control

and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks. Today, there is tremendous interest in VPNs over the Internet, especially due to the constant threat of hacker attacks. The VPN adds that extra layer of security, and a huge growth in VPN use is expected. In general, the different VPN solutions can be categorized into two main groups; customer premises equipment (CPE) based solutions or network based solutions.

Internet is a public data network based on network paradigms such as equal and best effort traffic treatment. All traffic crossing the Internet is public and insecure resulting in a number of problems that need to be solved, e.g. end-to-end security communication between enterprise sites. Some problems have solutions supported by several VPN system vendors, such as encrypted IP tunnelling between end-users using the IPSec architecture described by S. Kent and R. Atkinson in "Security Architecture for the Internet Protocol", RFC 2401, November 1998, or stand-alone firewall solutions, desktop software VPN clients. e.g. Microsoft® VPN, etc. A PC that is connected to Internet can, not easily but it is possible, be used as a transit node by a hacker, e.g. the hacker could use a Trojan horse program to get inside the PC. Well inside, the Trojan horse program may be adapted to release application software that will act as some authenticated software installed by the owner of the PC. It is very difficult for layer 2 and 3 firmware/software to detect this kind of malicious applications. Therefore, it is recommendable to have VPN control and management software and firmware functions and end-user applications, such as service login software, "authenticated" software applications that in some way uses the network infrastructure provided by the VPN service, separated on different hardware platforms. What generally should be avoided, is having PC clients that are responsible for configuring the actual VPN setup, i.e. having access to the lookup-table for other VPN members public IP addresses, having access to information on how to authenticate, perform integrity check and encrypt traffic aimed for the VPN etc.

Normally, users connected to the Internet are only limited in their use of services by how their firewall accepts or declines the use of distributed services. In order to be able to access a certain service, firewall settings need to be changed, and permissions are granted for the specific configuration setting that map to the service to which access is needed. A problem arises when users are connected to a Virtual Private Network (VPN), where services outside the VPN are inaccessible to the user, due to the logical separation of the VPN and the physical network. In a way, the separation of the VPN from the physical network can be seen as a firewall configured to block all traffic between the two networks. Services outside the VPN are inaccessible from within the VPN, and vice versa. Any service that needs to be

accessed from within a VPN may be

- an integrated part of the VPN, e.g. a DHCP server within the VPN driver of the client system, DHCP (Dynamic Host Configuration Protocol) being a software that automatically assigns IP addresses to client stations logging onto an IP network. This is a commonly used way of assigning IP addresses dynamically to hosts on the local network. Normally, each client computer receives a free IP address when booting. This address then has to be renewed with a time interval, to ensure that the DHCP server does not run out of free addresses;
- inside the VPN, running as a normal service on a server connected to the VPN;
- outside the VPN, i.e. normally inaccessible from the VPN;
- any other service that could provide a feature to the users of the VPN.

There is normally no way of providing easy access to all kinds of services within or outside the VPN, since there exists no way to map services to their logical representation in a way that is useful for a user of the VPN. A service might be inside, outside, or an integral part of the VPN system, and in practice, these differences make the configuration of services hard work for the systems administrator.

Summary of the invention

According to first aspect the invention relates to a system for providing a service to a client in a virtual network, which virtual network resides on but is logically separated from a physical network. In said system a network service is located in a server, and a logical representation of the network service is provided. This logical representation is connected to the virtual network by a virtual administrative interface.

Preferably said logical representation includes a mapping to the network service, thereby representing a virtual service accessible to said client.

According to an embodiment of the invention said logical representation makes said network service replaceable without changing configuration of the virtual network system. Preferably said service is configured to be experienced by said client as a part of the virtual network.

Said network service may be a service running on the server, currently connected to the virtual network. In such case, said logical representation is preferably directly connected to said server. Alternatively, said network service is a service running on the server, which server is located outside the virtual network, where special access rules define how the server might be accessed and by whom. In such case, the logical representation is connected to said server through said

physical network.

In one embodiment said virtual administrative interface is configured to allow client users to perform predetermined administrative functions themselves, such as subscribing/unsubscribing themselves to certain services. Preferably said physical network is an Internet Protocol network.

According to a second aspect of the invention, a method is provided for taking the steps described in this application, for providing virtual services in a virtual private network.

Brief description of the drawings

Preferred embodiments of the invention are described below with references being made to the drawings, on which

Fig. 1 illustrates the system overview according to an embodiment of the present invention;

Fig. 2 illustrates traffic monitoring and session overtaking according to an embodiment of the present invention;

Fig. 3 illustrates the logical representation of services for a virtual network, according to an embodiment of the invention; and

Fig. 4 illustrates the connection between the actual service and the interface towards clients of the virtual network, according to an embodiment of the present invention.

Fig. 5 illustrates an emulated LAN on top of a global IP network, according to an embodiment of the invention.

Detailed description of preferred embodiments

According to one aspect, the system according to the present invention is based on a standard IP network like the public Internet. The system comprises multiple VPN clients and at least one server. One server can be a distributed cluster of physical boxes. The VPN clients could be implemented as drivers on the client computer but are for security reasons preferably implemented in a stand alone hardware box. A purpose of this mechanism is to establish dynamic and secure Virtual Local area Networks between some or all of the clients. A virtual network is created by establishing connection groups in a VPN server. The server has a service device for keeping track of connected machines and mapping them to IP addresses. In one embodiment this is obtained using ARP (Address Resolution Protocol), an IP protocol used to obtain a node's physical address. A client station sends an ARP request to the VPN server with the VPN internal IP address of the target node it wishes to communicate with, and the VPN server responds by sending back the

external IP address so that packets can be transmitted. ARP returns the layer-2 address for a layer-3 address. This mechanism also handles distribution of public keys to form complete security associations. For handling broadcasts an emulated broadcast service is implemented in the server, preferably using an IP multicast group or as a separate broadcast service. Data sent directly from one machine in the virtual network to another is tunnelled over IP directly to the IP address of the receiving client. The mechanism includes both the case where data packets are tunnelled directly over IP and when an layer-2 media such as Ethernet is bridged onto the IP network.

Fig. 5 illustrates an embodiment of the system according to the present mechanism, wherein a network 4 comprises five nodes; four VPN clients 31 - 34 with global addresses C1 - C4, and a server S. All of these are connected to and have a valid address in the physical network 4. These nodes are interconnected using standard Internet routing procedures, but the clients 31 - 34 are not on the same LAN. On top of this network infrastructure, clients 31, 32 and 33 form a virtual network 30 with local addresses D1, D2 and D3. In the illustrated case the clients in this VPN appear to be on the same local area network. The reason for this is the broadcast service, i.e. the service device, which delivers all packets for the local broadcast domain to all machines on the VPN 30. Thus service discovery mechanisms or layer-2 ARP operate transparently on top of the virtual network. When client 31 on the VPN wants to transmit a packet directly to client 32 the client-software requests the physical address C2 from server S, based upon the local address D2, and possible security keys required for talking to D2 from S. D1 is then able to transmit the packet in a secure tunnel directly to D2 without passing the server S.

The above provides an effective and user friendly mechanism for establishing Virtual Private Networks over generic IP connections. Broadcast services and service discovery protocols that normally require a direct layer-2 interconnection may work independently of the actual network structure. It also provides the possibilities of distributed network broadcast handling, where rules and configuration options may be cached in the end nodes of the network instead of in a centralised server. The described mechanism is unique in that it presents a complete distributed emulated LAN on top of an IP network where access and attributes such as security associations are completely controlled by a server. Most current solutions uses static tunnels. Either permanent connections are set up between the members of the VPN or tunnel servers which basically works as modem pools only you "dial" an IP number. This means that all traffic no matter it's final destination goes through this one box. In particular traffic going to sites in the VLAN (Virtual LAN) other than that of the VLAN server comes in through the server access and turns. The

broadcast service allows service discovery protocols designed for local networks to function on the VPN while the ARP mechanism allows for dynamic establishment of secure tunnels directly between endpoints. The well known LANE (LAN Emulation) standard was focused entirely on ATM (Asynchronous Transfer Mode) and featured no integrated security handling. Lane introduces, inter alia, the ability to connect Ethernet and Token Ring networks together via ATM. LANE makes the process transparent, requiring no modification to Ethernet and Token Ring stations. LANE allows common protocols, such as IP, IPX, AppleTalk and DECnet, to ride over an ATM backbone. LAN emulation has been implemented and verified over ATM. However, since the system architecture itself by design avoids sending all data through the server, the bottleneck problem with overloaded server links is completely avoided.

In general, the target system relies on a decision scheme for a third-party overtaking of a client role in a two-party communication session. Turning to Fig. 1, the system processes comprises end user clients located at the end user premises equipment 1, a central VPN system server 2, and network edge located VPN system clients 3. Full lines indicate physical communication lines, whereas arrows indicate communicating ends, without specifying which route the communication takes between those communicating ends. As previously described VPN is a commonly used term to describe a logical network residing on top of an actual, physical network, or networks. To the users and client applications, the logical network behaves just like a normal network, but the networks perimeters and boundaries are not specified by a physical or network-based topology, but by a logical description of its rules and components

The end user client process preferably resides in a PC, the VPN client process preferably resides within a standalone hardware unit, and the VPN server process resides within any kind of Server hardware unit, such as an IBM® Server. By process is here meant the functionality for the particular client or server, as described herein. The VPN server 2 and the VPN client 3 are parts of a VPN system that provides the end user client 1 with access to required VPNs. The end user client 1 hardware is physically connected via a communication line 11 to the VPN client 3 hardware. The VPN client 3 hardware is physically connected to a layer-two termination that enables the VPN client 3 to access Internet over a communication line 12. The layer-two protocol is preferably Ethernet but could practically be any known layer-two protocol used for the encapsulation and transport of IP (Internet Protocol) packets between IP nodes. The VPN server 2 is connected to Internet via a communication line 13 in the same way as the VPN client 3.

According to an embodiment of the target system the end user client 1 initiates a communication session with the VPN server 2 in order to acquire access to a

virtual private network. During the initialisation phase, the VPN server 2 authenticates and authorizes the end user client 1 as a registered user of VPN services that are provided by the VPN server 2. The VPN client 3 is passive in that it does not initiate any new information elements during the initialisation phase. The VPN client 3 also monitors 22 the communication 21 between the end user client 1 and the VPN server 2.

When the initialisation phase between the end user client 1 and the VPN server 2 is finished, and when information has been exchanged, regarding particular VPN that the end user clients request access to, then the VPN client 3 becomes active and takes over the communication session between the end user client 1 and the VPN client 3. The VPN client 3 now requests, if it is necessary because the VPN information can already be cached by the VPN client 3, VPN configuration data from the VPN server 2. The VPN client 3 uses the configuration data to configure necessary VPN access parameters such as traffic classification parameters, performance assurance parameters, or firewall parameters such as encryption, authentication, filtering parameters, etc.

The end user client 1 is allowed to use different VPN servers 2 but cannot have simultaneous access to more than one VPN server 2. The VPN client 3 detects when an end user client 1 tries to access a certain server 2. At this moment the VPN server 2 is considered insecure until the end user client 1 has authenticated the VPN server 2 and also have been authenticated by the VPN server 2.

The monitoring and session overtaking scenarios are described more in detail in Fig. 2. The VPN client 3 has one trusted domain, which is the end user client 1 side, and one distrusted domain, the Internet domain. From the VPN client's 3 point of view, the VPN server 2 is therefore located in the distrusted domain. Since all in- and outgoing IP traffic to/from the end user client passes through the VPN client 3 hardware, the VPN client 3 is able to monitor the communication 21 between the end user client 1 and the VPN server 2. This is true if, and only if, the IP traffic not is encrypted in such a way that the VPN client 3 is unable to decrypt the IP traffic. The VPN client 3 software resides on hardware that physically interconnects the end user client 1 with Internet 4. The VPN client 3 is therefore able to monitor 22 all traffic 21 between the end user client 1 and different VPN servers 2 to whom the end user client 1 are registered as user.

The VPN client 3 identifies when the end user client 1 starts to establish contact with a VPN server 2. The VPN client 3 treats the end user client 1 side as a trusted party and the VPN server 2 as a distrusted party. The session establishment phase 21 between the end user client 1 and the VPN server 2 could be done in numerous ways, e.g. by a traditional challenge/response handshaking sequence. The communication 21 is primarily meant to be done by web based clients but other

client/server process environment solutions are possible. When the handshaking sequence between the end user client 1 and the VPN server 2 has finished, the VPN client 3 takes over the communication session. The handshaking is considered finished when the VPN server 2 has authenticated and authorised the end user client 1, and acknowledged the end user client 1 as a confirmed user. The VPN client 3 will from now on undertake proxy roles towards both the end user client 1 and the VPN server 2. Towards the end user client 1, the VPN client 3 will act as a VPN server proxy, and towards the VPN server 2 as an end user client proxy. The end user client 1 will continue it's session in belief that it still communicates with the VPN server 2. The VPN client 3 will, using the VPN server proxy role, continue the VPN setup session with the end user client 1.

Further on, the VPN client 3 is now considering the VPN server 2 as a secure source and starts up communication sessions 23 with the VPN server 2 that enables the end user client 1 to be included as members in the requested VPN.

In one embodiment the target system is implemented in a service provisioning system, where parts of the service functionality are distributed to system clients acting as server proxies. One technical advantages of the present system is that any hacker intrusions via an end user PC 1 are avoided by having critical software/firmware for control and management of VPN configuration data separated on standalone hardware 3. Another advantage is the automated overtaking of certified sessions. Another benefit is the plug-and-play behaviour for virtual services over Internet, which is made available through the system. The teachings of the present system thus differs from prior art technology, since earlier solutions to the problem have either been centralised server solutions, such as PSTN/ISDN modem-pool solutions, server centralised IP Sec tunnelling etc, or distributed solutions, which are only valid within one network operator intra-domain or within federated network operator domains. These solutions are generally referred to as network based VPN systems. The present system will function independently of whether or not the different VPN client users access the same network operator domain or a federated network domain or have access to totally independent network operator domains.

The present invention solves the problem of having strict boundaries and rules for what a service is supposed to be in a VPN. By applying the concept of virtual services as a mapping to an actual service, the complex structures of networked services are hidden from the users of the VPN, who still can pick and choose from what services they want to utilise in their own view of the network. By virtual service is here meant that that for the clients of the virtual network who access the service will experience the service as being a part of the emulated network, and will only experience the logic of the service. The actual service may however be located

outside the VPN. For administrators, the benefits are that the administrative interfaces for a service stays the same, even if the service itself is replaced with a different actual implementation of the service.

An example of an embodiment of the present invention is illustrated in Fig. 3, wherein dashed lines indicate connections in the virtual private network 30, and full lines indicate connections to the global network 4, preferably an IP network. In the disclosed embodiment the service "DHCP server", for example, may reside on a physical server machine S1 arranged and accessible inside the VPN 30, according to the prior art. According to the invention, it would also be possible to implement it in the control logic of the VPN instead, which normally would change the way configuring the DHCP server should be done. If a DHCP server S2 has a logical representation Logrep-S2 as well as a virtual administrative interface I-S2, the underlying service S2 could be replaced without changing the way the system administrator configures the system.

The system according to the present invention uses a concept where a network service, be it an access method or access rule or any IP/ IPv6 service, is represented as a sub-component S2,S3 of the VPN itself, and therefore may be added or removed from the VPN in a very intuitive way, e.g. using a drag-and-drop scheme, or using a simple set of configuration options in a configuration file. The Virtual service is configured to be seen as a part of a VPN, but it's corresponding actual service might be:

- an integrated service in the VPN technology used;
- a service running on a machine S2 currently connected to the VPN;
- a service running on a server S3 outside the VPN, where special access rules define how it might be accessed and by whom;
- any service to which there could exist a mapping that would let it appear as if it is part of the VPN itself.

As illustrated in Fig. 3, a service located on such a server S3 which is connected to the global network 4, e.g. the Internet, but which is not part of the VPN 30, may be used by the VPN clients C1,C2, by making use of the present invention. A logical representation Logrep-S3 provides the virtual service, and is mapped to the actual service in S3. The logical representation Logrep-S3 is connected to a virtual administrative interface I-S3, making it accessible for the VPN clients C1,C2. This embodiment too has the benefit of making replacements in the actual service without having to change the way the system administrator configures the system.

Fig. 4 illustrates schematically how a service is made available to a client of the VPN. The actual service is represented by a Virtual Service Logical representation, to which an administrative interface is bound. The administrative

interface may be set up to allow users to perform some administrative functions themselves, such as subscribing/unsubscribing themselves to certain services.

The invention may be used in any VPN technology that allows the administrators of the VPN to define access rules per networked service. There also has to exist a way to map a service definition within the VPN to generic services that might or might not exist within the VPN. The logical mapping between the Virtual Service and the actual service allows easy administration of services for the VPN administrators. The logical mapping could also be used to provide a common interface to the services, providing a "single sign-on" functionality. When configuring multiple services or servers, each service normally uses its own authentication scheme. A single sing-on scheme lets the administrator sign on once to a common authentication service, which then is used to authenticate the user to all other services.

The system according to the present invention differs from earlier known technology in that normally, a VPN is seen a network strictly detached from the underlying physical network, i.e. the global network as seen in Fig. 3. By allowing exceptions from this rule, where the exceptions are part of the VPN control logic, services and their access methods may be defined within the VPN configuration structure itself. This, in turn, allows for the possibility of defining a high level abstraction of what really defines a service, in a way that makes VPN configuration and management much more manageable. This provides a unified view for every service, independent of the actual service implementation. Also, the modular control architecture enables dynamic bundling of user specific services on top of the basic VPN service.

Claims

1. System for providing a service to a client (C1,C2) in a virtual network (30) residing on but being logically separated from a physical network (4), in which system a network service is located in a server (S2,S3), **characterised in** that a logical representation (L-S2,L-S3) of the network service is provided, and connected to the virtual network by a virtual administrative interface (I-S2,I-S3).

2. The system as recited in claim 1, wherein said logical representation includes a mapping to the network service, thereby representing a virtual service accessible to said client.

3. The system as recited in claim 2, wherein said logical representation makes said network service replaceable without changing configuration of the virtual network system.

4. The system as recited in claim 2, wherein said service is configured to be experienced by said client as a part of the virtual network.

5. The system as recited in claim 4, wherein said network service is a service running on the server (S2), currently connected to the virtual network.

6. The system as recited in claim 5, wherein said logical representation (L-S2) is directly connected to said server (S2).

7. The system as recited in claim 4, wherein said network service is a service running on the server (S3), located outside the virtual network, where special access rules define how the server might be accessed and by whom.

8. The system as recited in claim 7, wherein said logical representation (L-S3) is connected to said server (S3) through said physical network.

9. The system as recited in claim 2, wherein said virtual administrative interface is configured to allow client users to perform predetermined administrative functions themselves, such as subscribing/unsubscribing themselves to certain services.

10. The system as recited in any of the previous claims, wherein said physical network is an Internet Protocol network.

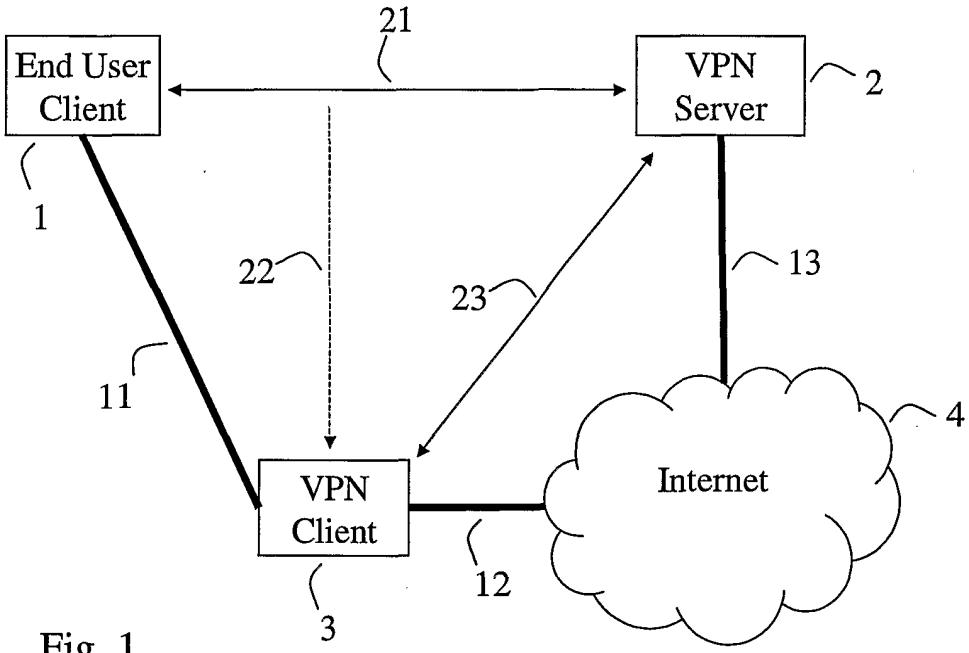

21
End User Client
VPN Server
2
1
22
23
13
11
4
Internet
VPN Client
12
3

Fig. 1

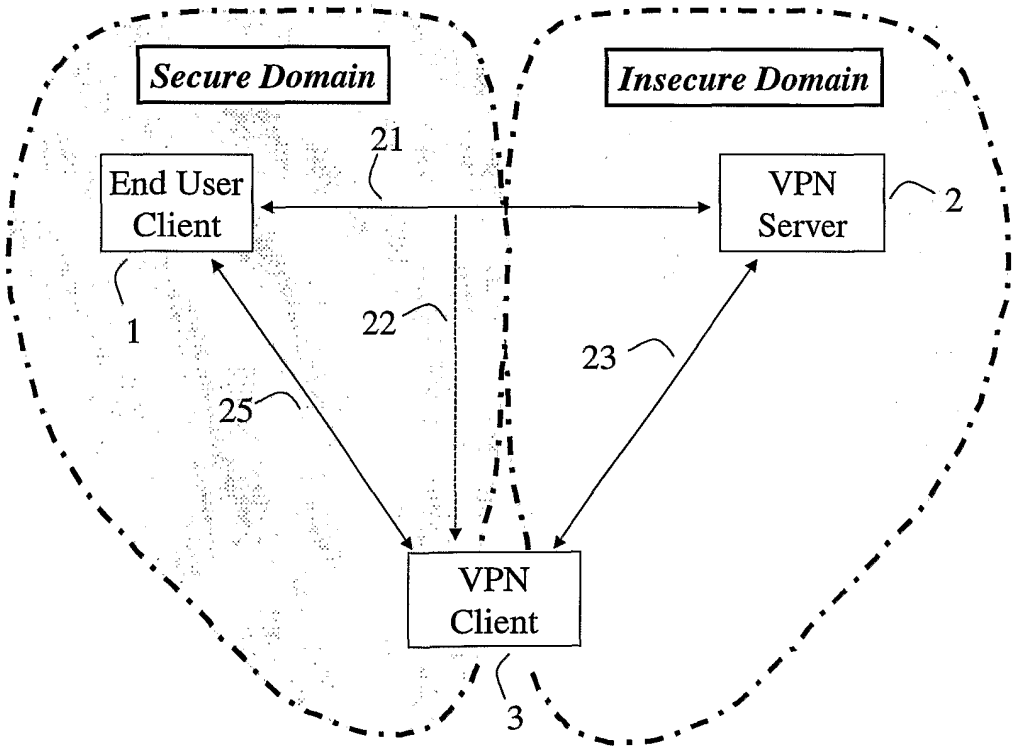

Secure Domain
Insecure Domain
21
End User Client
VPN Server
2
1
22
23
25
VPN Client
3

Fig. 2

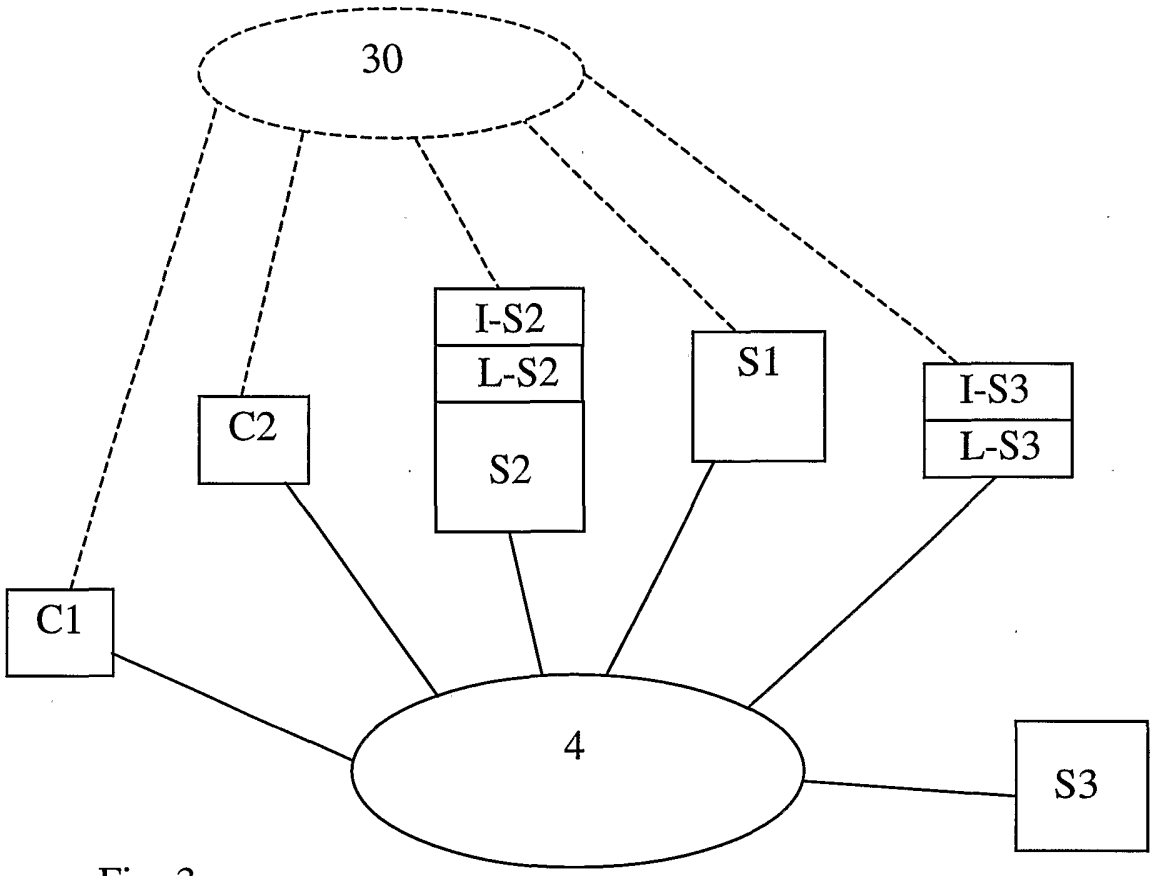

30
I-S2
L-S2
S2
S1
I-S3
L-S3
C2
C1
4
S3

Fig. 3

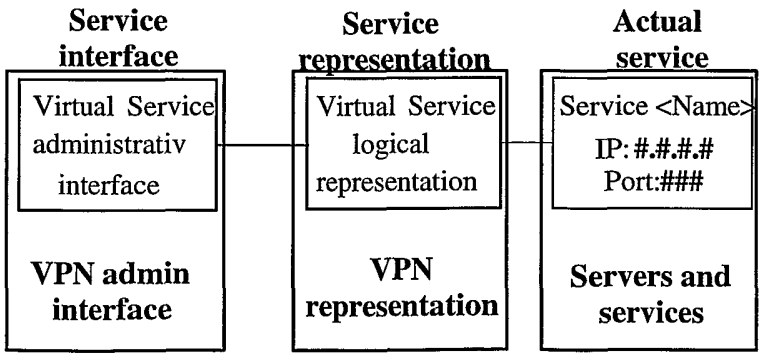

Service interface
Virtual Service administrativ interface
VPN admin interface
Service representation
Virtual Service logical representation
VPN representation
Actual service
Service <Name>
IP: #.#.#.#
Port:###
Servers and services

Fig. 4

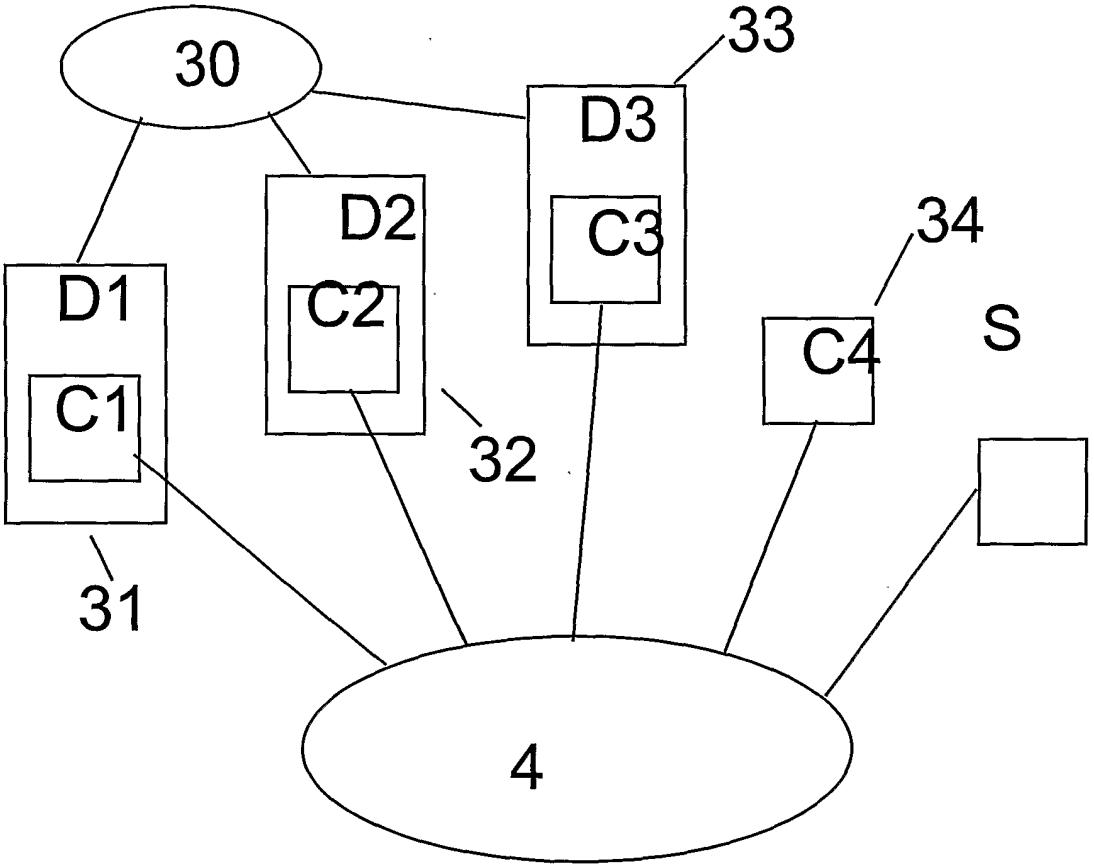


Fig 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01474

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/46
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)

IPC7: H04L, G06F

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

SE,DK,FI,NO classes as above

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

WPI DATA, EPO-INTERNAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6158011 A (CHEN,J.F.ET AL), 5 December 2000 (05.12.00), column 6, line 1 - line 50; column 8, line 37 - line 56; column 9, line 58 - line 64, figure 6, abstract ---	1-10
X	WO 0143392 A2 (SUN MICROSYSTEMS, INC), 4 June 2001 (04.06.01), page 5, line 2 - line 26; page 6, line 4 - line 19; page 7, line 15 - line 21, page 8, line 26 - line 30; page 14, line 3 - line 30, figure 3, abstract ---	1,2,4-6,9-10
A	EP 1093254 A2 (NORTEL NETWORKS LIMITED), 18 April 2001 (18.04.01), column 3, line 29 - column 4, line 14, figure 1, abstract ---	1-10

[X] Further documents are listed in the continuation of Box C. [X] 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
23 January 2002	29-01-2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Kristoffer Ogebjer/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01474

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6092200 A (MUNIYAPPA,U. ET AL), 18 July 2000 (18.07.00), column 1, line 5 - column 4, line 56, figure 1, abstract -- --------	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/02

International application No.
PCT/SE 01/01474

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6158011 A	05/12/00	AU 8915298 A	16/03/99
		US 6061796 A	09/05/00
		WO 9911019 A	04/03/99
WO 0143392 A2	04/06/01	AU 4310901 A	18/06/01
EP 1093254 A2	18/04/01	NONE	
US 6092200 A	18/07/00	NONE	