US 20010009025A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2001/0009025 A1

Ahonen (43) Pub. Date: Jul. 19, 2001

(54) **VIRTUAL PRIVATE NETWORKS**

(76) Inventor: **Pasi Matti Kalevi Ahonen**, Oulu (FI)

Correspondence Address:
Ronald L. Grudziecki
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404 (US)

(21) Appl. No.: **09/764,661**

(22) Filed: **Jan. 18, 2001**

(30) **Foreign Application Priority Data**

Jan. 18, 2000 (GB) 0000961.3

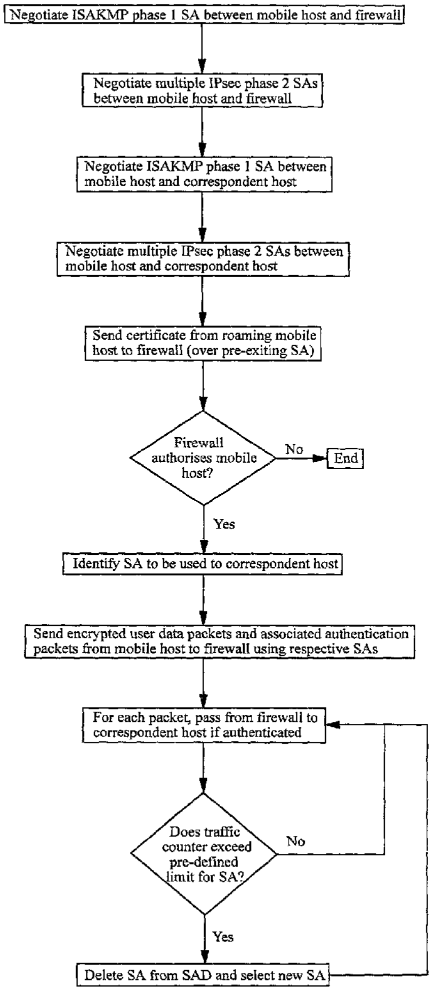
Publication Classification

(51) **Int. Cl.**^{7} **H04L 12/22**; H04L 9/00

(52) **U.S. Cl.** **713/161**; 713/151; 713/201

(57) **ABSTRACT**

A secure communication method for allowing a mobile host **1** to communicate with a correspondent host **4** over a Virtual Private Network. The method comprises negotiating one or more Security Associations (SAs) between the mobile host **1** and a correspondent host **4** of a Virtual Private Network (VPN). Subsequently, a communication is initiated between the mobile host **1** and a SG **3** and an authentication certificate sent to the SG **3,** the certificate containing at least the identity of a SA which will be used for subsequent communication between the mobile host and the correspondent host. Data packets can then be sent from the mobile host **1** to the correspondent host **4** using the identified SA, via the SG **3.** However, the data packets are forwarded by the SG **3** to the correspondent host **4** only if they are authenticated by the SG **3.**


Negotiate ISAKMP phase 1 SA between mobile host and firewall
Negotiate multiple IPsec phase 2 SAs between mobile host and firewall
Negotiate ISAKMP phase 1 SA between mobile host and correspondent host
Negotiate multiple IPsec phase 2 SAs between mobile host and correspondent host
Send certificate from roaming mobile host to firewall (over pre-exiting SA)
Firewall authorises mobile host?
No
End
Yes
Identify SA to be used to correspondent host
Send encrypted user data packets and associated authentication packets from mobile host to firewall using respective SAs
For each packet, pass from firewall to correspondent host if authenticated
Does traffic counter exceed pre-defined limit for SA?
No
Yes
Delete SA from SAD and select new SA

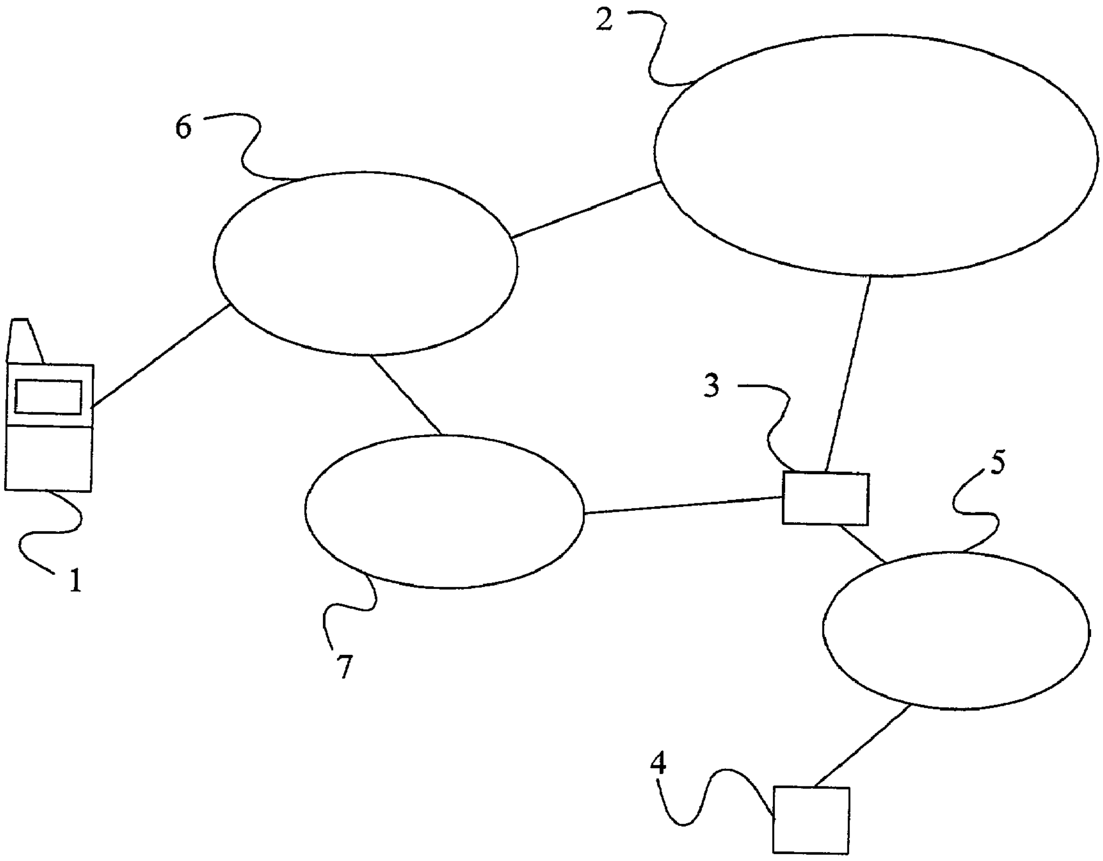


Figure 1

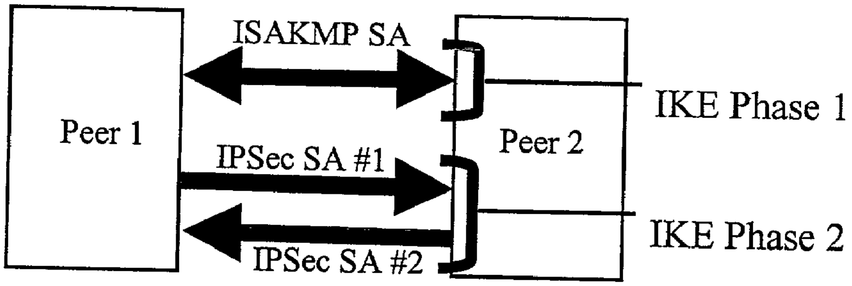


Figure 2

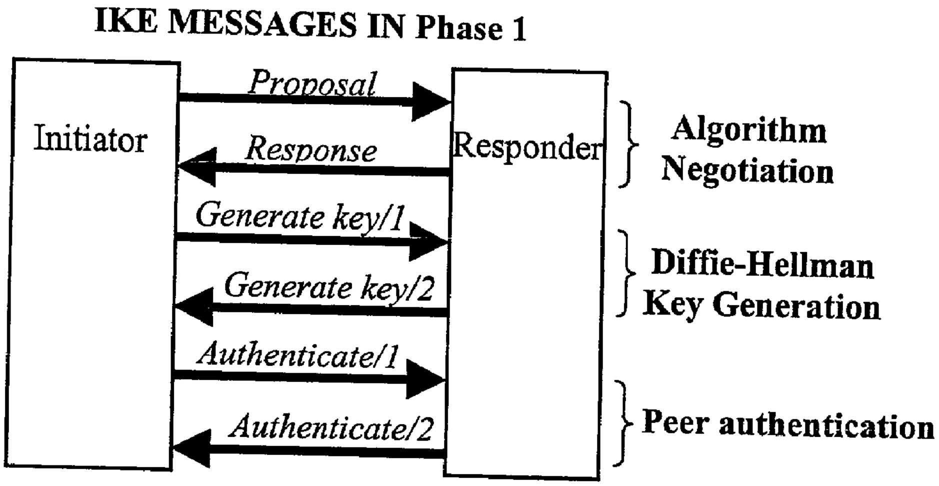


Figure 3

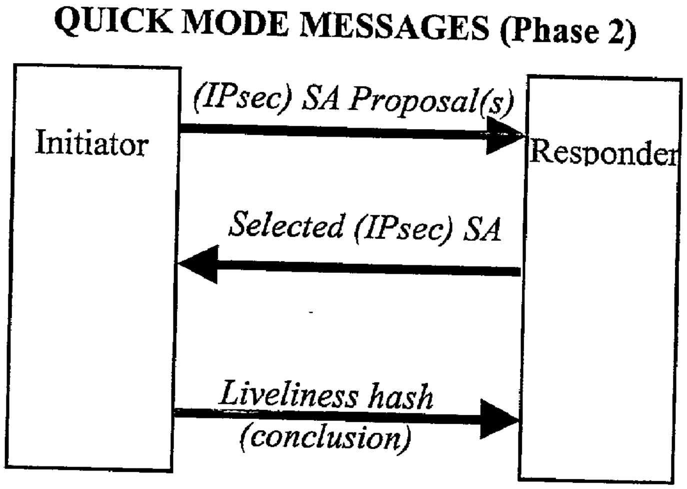


Figure 4

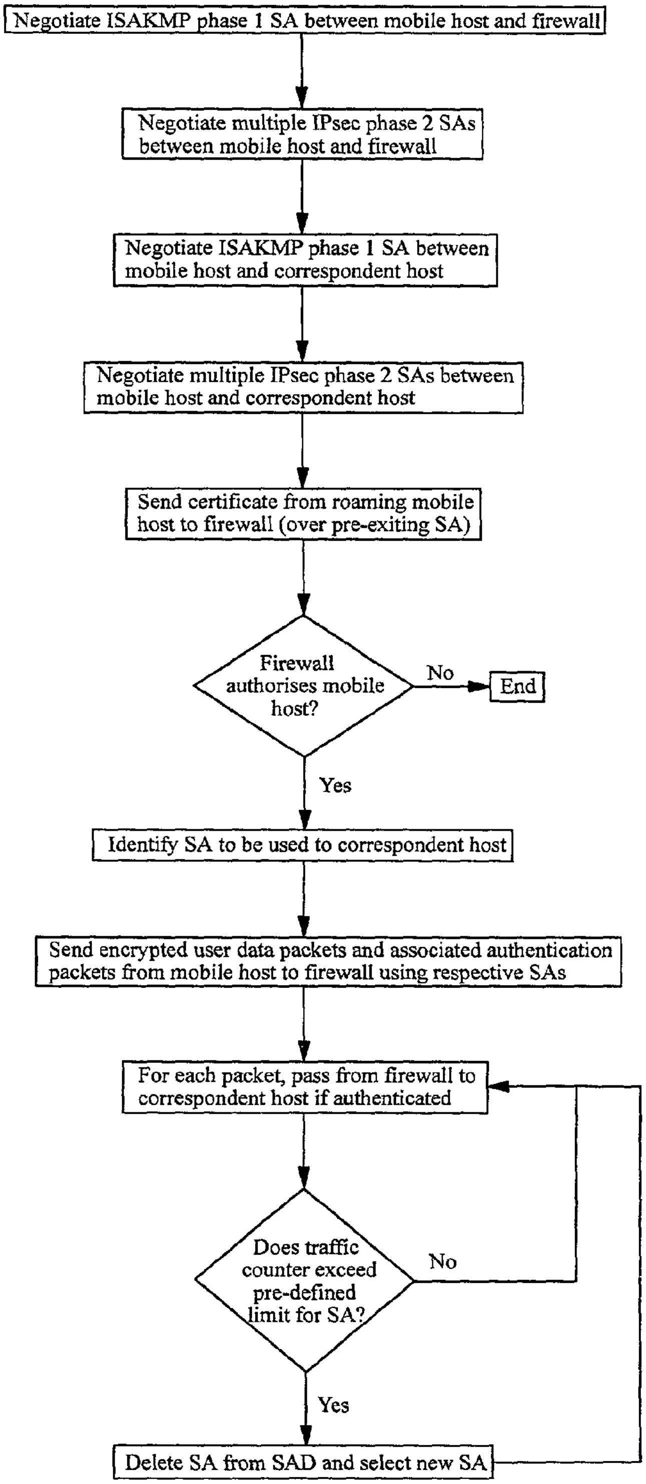

Negotiate ISAKMP phase 1 SA between mobile host and firewall
Negotiate multiple IPsec phase 2 SAs between mobile host and firewall
Negotiate ISAKMP phase 1 SA between mobile host and correspondent host
Negotiate multiple IPsec phase 2 SAs between mobile host and correspondent host
Send certificate from roaming mobile host to firewall (over pre-exiting SA)
Firewall authorises mobile host?
No
End
Yes
Identify SA to be used to correspondent host
Send encrypted user data packets and associated authentication packets from mobile host to firewall using respective SAs
For each packet, pass from firewall to correspondent host if authenticated
Does traffic counter exceed pre-defined limit for SA?
No
Yes
Delete SA from SAD and select new SA

Figure 5

VIRTUAL PRIVATE NETWORKS

FIELD OF THE INVENTION

[0001] The present invention relates to Virtual Private Networks and in particular to Virtual Private Networks in which a mobile terminal establishes a secure connection with a correspondent host located in an intranet, via a Security Gateway.

BACKGROUND OF THE INVENTION

[0002] There is an ever increasing demand for mobility in communications systems. However, this demand must be met in a manner which provides for the secure transfer of data between communicating parties. A concept known as the Virtual Private Network (VPN) has recently been introduced, with the aim of satisfying, by a combination of encryption and secure access, this demand. A VPN may involve one or more corporate Local Area Networks (LANs) or intranets, as well as users coupled to "foreign" LANs, the Internet, wireless mobile networks, etc.

[0003] An Internet Engineering Task Force (IETF) standard known as IPsec has been defined and provides for the creation of a secure connection between parties in a VPN over IPv6. In the IPsec model the end points of the secure connection are identified by their IP addresses. Whilst this may be satisfactory for users having a fixed connection, it does present problems for the mobile user (such as a user who connects to the VPN via a wireless terminal) who wishes to roam between different access networks. The main problem is that the IP address allocated to the roaming mobile user is likely to change dynamically as the user moves between access networks. In the event of an IP address change, it is difficult to reuse the pre-existing security associations (of IPsec) and in the worst case scenario the communicating parties need to make a re-authentication of one another and establish new security associations on the basis of the new IP address(es). This will result in increased signalling traffic and will degrade the performance of the VPN and of the applications being run.

SUMMARY OF THE INVENTION

[0004] According to a first aspect of the present invention there is provided a secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network via a Security Gateway (SG), the method comprising the steps of:

[0005] (1) negotiating one or more Security Associations (SAs) between the mobile host and a correspondent host of a Virtual Private Network (VPN);

[0006] (2) subsequently initiating a communication between the mobile host and the SG and sending an authentication certificate to the SG, the certificate containing at least the identity of a SA which will be used for subsequent communication between the mobile host and the correspondent host;

[0007] (3) sending data packets from the mobile host to the correspondent host using the identified SA, via the SG; and

[0008] (4) wherein said data packets are forwarded by the SG to the correspondent host only if they are authenticated by the SG.

[0009] Preferably, prior to step (2) of the above method, one or more Security Associations (SAs) are negotiated between the mobile host and the SG and said authentication certificate is sent to the SG using one of these SAs.

[0010] Preferably, the authentication certificate sent to the SG contains an IP address of the mobile host. This may be required, for example, when the mobile host has been allocated a new IP address.

[0011] Preferably, said SAs are IPsec phase **2** SAs and are used on top of an ISAKMP SA. More preferably, said authentication certificate contains the ISAKMP cookies of the mobile host and said correspondent host, with which the phase **2** negotiation was done.

[0012] Embodiments of the present invention reduce the amount of security related messaging during on-the-fly IP address changes, as the SAs needed to provide for secure communication between the mobile host and the correspondent host pre-exist. When it is required to initiate a new communication, it is only necessary for the mobile host to authorise the SG to forward packets belonging to a certain SA between the mobile host and said correspondent host.

[0013] Preferably, the VPN comprises an intranet, with the SG being coupled between the intranet and the Internet. The SG may also be coupled between the intranet and another network such as a core network of a mobile wireless telecommunications system (such as UMTS).

[0014] The mobile host may be a wireless host coupled to the SG via an access network, which may be an access network of a mobile wireless telecommunications system (for example the UTRAN access network of UMTS) or a wireless LAN or WAN. Said correspondent host may also be a mobile host, or it may be a fixed host.

[0015] In the case where the VPN comprises an intranet, said correspondent host may reside within the intranet, or may reside outside of the intranet. In the later case, said data packets are forwarded to the correspondent host from the SG over a secure connection. This may be established in the same way as the secure connection between said mobile host and the SG.

[0016] In certain embodiments of the present invention, a negotiated SA expires after a predefined volume of data has been sent using the SA. The SG maintains a record of the sent data volume and suspends the SA when the predefined volume is reached.

[0017] In certain embodiments of the invention, a negotiated SA is time limited by the SG. At the end of a predefined time limit the SA identity is suspend by the SG.

[0018] In the case of cellular access, the data packets sent to the SG in step (3) and which contain user data are authenticated using authentication data sent in separate data packets. For example these separate data packets may contain hashes of the user data. More preferably, the data packets containing user data are sent (possibly encrypted) using a Security Association (SA) negotiated between the mobile host and said correspondent host and the data packets containing authentication data are sent using Security Associations (SA) negotiated between the mobile host and the SG.

[0019] According to a second aspect of the present invention there is provided a Security Gateway (SG) of a Virtual

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.