Abstract: A solution is provided wherein a VPN session may be suspended without termination. When a user wishes to connect to a host outside of the VPN, the device does not abandon the secure connection. Instead, it stores all the necessary network parameters associated with the secure VPN connections for later recall. When the user later wishes to connect to the VPN again, the device may then simply recall the necessary network parameters associated with the prior secure VPN connection, and begin data transfer with the VPN.
Published:
— without international search report and to be republished upon receipt of that 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.
SPECIFICATION

TITLE OF INVENTION
SUSPENSION AND RESUMPTION OF SECURE DATA CONNECTION SESSION

BACKGROUND OF THE INVENTION

[0001] The present invention relates to the field of computer networking. More specifically, the present invention relates to the suspension and resumption of a secure data connection session in a computer network.

[0002] In the field of computer networking, virtual private networks (VPNs) have grown quite popular with enterprises wishing to provide secure access to a private network. VPN is a wide area network that connects private subscribers (for example, employees of the same company) together using the public Internet as the transport medium, while ensuring that their traffic is not readable by the Internet at large. All the data is encrypted to prevent others from reading it, and authentication measures ensure that only messages from authorized VPN users can be received.

[0003] The data encryption is handled through the exchange of keys upon negotiation of a virtual private network link, also known as a tunnel. The generation of keys, however, is time consuming, interrupts user processes, and is generally processor-hungry. It is therefore beneficial to reduce the number of times keys will have to be generated.

[0004] Another problem with current VPN solutions is that, upon gaining access to a secure private network, the user is now exclusively blocked from accessing other networks. For instance, a user cannot access a Multimedia Messaging Service (MMS) gateway that is behind their carrier or Internet Service Provider's network, or access the Internet. In order for a user to access such networks, he must shut down the VPN tunnel, then later bring it back up once he is finished accessing the other networks. Additionally, if the user device is a handheld computer, the tunnel has to be brought down if another IP address is brought up, for instance, the device is
This causes a need to re-negotiate the keys, and thus runs into the aforementioned problems involved with the generation of keys.

The result of this is that VPN sessions, which should be good for up to 18 hours, often need to be torn down after just 15 minutes. This adds additional burden to the processors in the network as well as to network bandwidth, as keys must be renegotiated and secure token codes re-entered each time the VPN session is reactivated.

In the past, this problem has been solved using split-tunneling, where multiple tunnels are kept open simultaneously. However, this creates fairly dramatic problems with Domain Name Service (DNS) lookups, as the device often will not know which tunnel to use for the lookup, and can cause ambiguous IP addresses to be simultaneously present.

FIG. t is a timing diagram illustrating the typical scenario where the user requests a connection to a VPN. On receipt of such a request, the VPN server obtains authentication information from the user and checks these against its Authentication, Authorization and Accounting (AAA) server. Once the user's credentials have been validated, the secure tunnel is established and the user's device sends and receives encrypted data with the VPN server. The VPN server in turn relays the data to and from the destination host on the VPN. When the user wishes to connect to a host outside of the VPN, the device abandons the secure connection with the VPN and connects to the non-VPN host directly. If the user wishes to connect to a host within the VPN again, it must now go through the entire process of validation/authentication with the VPN server and AAA server.

What is needed is a solution that allows a user to connect to a network outside of the VPN while maintaining a VPN session and without encountering the DNS problems of prior art solutions.
A solution is provided wherein a VPN session may be suspended without termination. When a user wishes to connect to a host outside of the VPN, the device does not abandon the secure connection. Instead, it stores all the necessary network parameters associated with the secure VPN connections for later recall. When the user later wishes to connect to the VPN again, the device may then simply recall the necessary network parameters associated with the prior secure VPN connection, and begin data transfer with the VPN.

The accompanying drawings, which are incorporated into and constitute a part of this specification, illustrate one or more embodiments of the present invention and, together with the detailed description, serve to explain the principles and implementations of the invention.

In the drawings:

Fig. 1 is a timing diagram illustrating the typical scenario where the user requests a connection to a VPN.

Fig. 2 is a timing diagram illustrating an embodiment of the present invention.

Fig. 3 is a timing diagram illustrating another embodiment of the present invention.

Fig. 4 is a flow diagram illustrating a method for managing a virtual private network session between a device and a VPN server in accordance with an embodiment of the present invention.

Fig. 5 is a flow diagram illustrating a method for managing a virtual private network session between a device and a first VPN server in accordance with another embodiment of the present invention.
FIG. 6 is a block diagram illustrating an apparatus for managing a virtual private network session between a device and a VPN server in accordance with an embodiment of the present invention.

FIG. 7 is a block diagram illustrating an apparatus for managing a virtual private network session between a device and a first VPN server in accordance with another embodiment of the present invention.
DETAILED DESCRIPTION

[0012] Embodiments of the present invention are described herein in the context of a system of computers, servers, and software. Those of ordinary skill in the art will realize that the following detailed description of the present invention is illustrative only and is not intended to be in any way limiting. Other embodiments of the present invention will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations of the present invention as illustrated in the accompanying drawings. The same reference indicators will be used throughout the drawings and the following detailed description to refer to the same or like parts.

[0013] In the interest of clarity, not all of the routine features of the implementations described herein are shown and described. It will, of course, be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made in order to achieve the developer's specific goals, such as compliance with application- and business-related constraints, and that these specific goals will vary from one implementation to another and from one developer to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

[0014] In accordance with the present invention, the components, process steps, and/or data structures may be implemented using various types of operating systems, computing platforms, computer programs, and/or general purpose machines. In addition, those of ordinary skill in the art will recognize that devices of a less general purpose nature, such as hardwired devices, field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

[0015] A solution is provided wherein a VPN session may be suspended without termination. When a user wishes to connect to a host outside of the VPN, the device does not abandon the
secure connection. Instead, it stores all the necessary network parameters associated with the secure VPN connections for later recall. When the user later wishes to connect to the VPN again, the device may then simply recall the necessary network parameters associated with the prior secure VPN connection, and being data transfer with the VPN.

[0016] FIG. 2 is a timing diagram illustrating an embodiment of the present invention. As can be seen in this figure, not only is the reconnection achieved with fewer message exchanges between the device and the VPN server, there is also no need for the user to supply the authentication credentials again. The exchange of new authentication credentials requires the establishment of new encryption keys, which is processor intensive and can be demanding on small portable devices. Elimination of these steps, therefore, is quite beneficial.

[0017] FIG. 3 is a timing diagram illustrating another embodiment of the present invention. In this case, rather than the user desiring to connecting to a host outside of a VPN, the user actually wants to change the connection from one VPN to another VPN. In this case, the present invention allows storage and retrieval of multiple sets of network parameters, each associated with a specific VPN. The reconnection with each VPN is made efficient with the ability to recall the necessary parameters. While this scenario may be a rare occurrence, this example illustrates the power and extensibility of the present invention.

[0018] The VPN parameters that need to be saved in these cases are only those parameters necessary to restart a VPN later. In a sense, the VPN parameters which are stored represent a "snapshot" of the established VPN. In one embodiment of the present invention, one of these parameters is a security association. The concepts of a security associate is fundamental to the IP Security Protocol (IPSec). A security association is a relationship between two or more entities that describes how the entities will use security services to communicate securely. IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, authentication, integrity, or all three services. When the security service is determined, the two IPSec peers must determine exactly which algorithms to use (e.g., MD5). After deciding on the algorithms, the two devices must share session keys. The
security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. It should be noted that while security associations are a key part of IPSec, security associations may apply to many different protocols. IPSec is merely one example of a secure access mechanism that is effective for the establishment of a VPN.

[0019] Each security association may comprise values such as destination address, a security parameter index, the IPSec transforms used for that session, security keys, and additional attributes such as IPSec lifetime.

[0020] FIG. 4 is a flow diagram illustrating a method for managing a virtual private network session between a device and a VPN server in accordance with an embodiment of the present invention. The method may be performed at the device. Each act of the method may be performed in hardware, software, or any combination thereof. At 400, a VPN session may be established between the device and the VPN server. At 402, a request to access a non-VPN host may be received from a user. In response to this, at 404, one or more VPN parameters for the VPN session may be stored on the device. These parameters may include a security association, a domain name service (DNS) server address, an IP address of the device, a default gateway, and/or a DNS server list. At 406, the VPN session may be suspended. This may include preventing a user of the device from accessing the VPN session without informing the VPN server of such prevention.

[0021] At 408, a non-VPN session between the device and the non-VPN host may be established. Once the user has finished accessing the non-VPN host, at 410, the non-VPN session may be terminated. Then, at 412, the VPN session may be resumed by retrieving the one or more VPN parameters for the VPN session from the device. This may include once again allowing the user of the device to access the VPN session, without informing the VPN server of any change in the access rights of the user.

[0022] FIG. 5 is a flow diagram illustrating a method for managing a virtual private network session between a device and a first VPN server in accordance with another embodiment of the
present invention. The method may be performed at the device. Each act of the method may be performed in hardware, software, or any combination thereof. At 500, a VPN session may be established between the device and the first VPN server. At 502, a request to access a second VPN may be received from a user. In response to this, at 504, one or more VPN parameters for the VPN session between the device and the first VPN server may be stored on the device. These parameters may include a security association, a domain name service (DNS) server address, an IP address of the device, a default gateway, and/or a DNS server list. At 506, the VPN session between the device and the first VPN server may be suspended. This may include preventing a user of the device from accessing the VPN session between the device and the first VPN server without informing the first VPN server of such prevention.

[0023] At 508, a VPN session between the device and a second VPN server may be established. Once the user has finished accessing the second VPN, at 510, one or more parameters for the VPN session between the device and the second VPN server may be stored on the device. These parameters may include a security association, a domain name service (DNS) server address, an IP address of the device, a default gateway, and/or a DNS server list. Then, at 512, the VPN session between the device and the second VPN server may be suspended. This may include preventing a user of the device from accessing the VPN session between the device and the second VPN server without informing the second VPN server of such prevention. Then, at 514, the VPN session between the device and the first VPN server may be resumed by retrieving the one or more VPN parameters for the VPN session between the device and the first VPN server from the device. This may include once again allowing the user of the device to access the VPN session, without informing the VPN server of any change in the access rights of the user.

10024] FIG. 6 is a block diagram illustrating an apparatus for managing a virtual private network session between a device and a VPN server in accordance with an embodiment of the present invention. The apparatus may be located at the device. Each element of the apparatus may be embodied in hardware, software, or any combination thereof. A VPN session establisher 600 may establish a VPN session between the device and the VPN server. A VPN parameter
storer 602 coupled to the VPN session establisher 600 may store one or more VPN parameters for the VPN session on the device. These parameters may include a security association, a domain name service (DNS) server address, an IP address of the device, a default gateway, and/or a DNS server list. A non-VPN host access request receiver 604 may receive a request to access a non-VPN host from a user. In response to this, a VPN session suspender 606 coupled to the VPN parameter storer 602 and to the non-VPN host access request receiver 604 may suspend the VPN session. This may include preventing a user of the device from accessing the VPN session without informing the VPN server of such prevention.

(0025J) A non-VPN session establisher 608 may establish a non-VPN session between the device and the non-VPN host. Once the user has finished accessing the non-VPN host, a non-VPN session terminator 610 coupled to said non-VPN session establisher 608 may terminate the non-VPN session. Then, a VPN session resumer 612 coupled to the VPN parameter storer 602 and to the non-VPN session terminator 610 may resume the VPN session by retrieving the one or more VPN parameters for the VPN session from the device. This may include once again allowing the user of the device to access the VPN session, without informing the VPN server of any change in the access rights of the user.

f0Q26J FIG. 7 is a block diagram illustrating an apparatus for managing a virtual private network session between a device and a first VPN server in accordance with another embodiment of the present invention. The apparatus may be located on the device. Each element of the apparatus may be embodied in hardware, software, or any combination thereof. A first VPN session establisher 700 may establish a VPN session between the device and the first VFN server. A first VPN parameter storer 702 coupled to the first VPN session establisher 700 may store one or more VPN parameters for the VPN session between the device and the first VPN server on the device. These parameters may include a security association, a domain name service (DNS) server address, an IP address of the device, a default gateway, and/or a DNS server list. A second VPN access request receiver 704 may receive a request to access a second VPN from a user. In response to this, a first VPN session suspender 706 coupled to the first VPN parameter storer 702 and to the second VPN access request receiver 704 may suspend the
VPN session between the device and the first VPN server. This may include preventing a user of the device from accessing the VPN session between the device and the first VPN server without informing the first VPN server of such prevention.

(0027) A second VPN session establisher 708 may establish a VPN session between the device and a second VPN server. Once the user has finished accessing the second VPN, a second VPN parameter storer 710 coupled to the second VPN session establisher 708 may store one or more parameters for the VPN session between the device and the second VPN server on the device. These parameters may include a security association, a domain name service (DNS) server address, an IP address of the device, a default gateway, and/or a DNS server list. Then, a second VPN session suspender 712 coupled to the second VPN parameter storer 710 may suspend the VPN session between the device and the second VPN server. This may include preventing a user of the device from accessing the VPN session between the device the second VPN server without informing the second VPN server of such prevention. Then, a first VPN session restorer 714 coupled to the first VPN parameter storer 702 and to the second VPN session suspender 712 may resume the VPN session between the device and the first VPN server by retrieving the one or more VPN parameters for the VPN session between the device and the first VPN server from the device. This may include once again allowing the user of the device to access the VPN session, without informing the VPN server of any change in the access rights of the user.

(0028) While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.
CLAIMS

What is claimed is:

1. A method for managing, at a device, a virtual private network (VPN) session between the device and a VPN server, the method comprising:
   - establishing a VPN session between the device and the VPN server;
   - storing one or more VPN parameters for the VPN session on the device;
   - suspending the VPN session;
   - establishing a non-VPN session between the device and a non-VPN host;
   - terminating said non-VPN session;
   - resuming the VPN session by retrieving said one or more VPN parameters for the VPN session from the device.

2. The method of claim 1, wherein said suspending includes preventing a user of the device from accessing the VPN session without informing the VPN server of such prevention.

3. The method of claim 1, wherein said one or more VPN parameters includes a security association.

4. The method of claim 3, wherein said one or more VPN parameters further includes at least one parameter selected from the group consisting of:
   - a domain name service (DNS) server address;
   - an IP address of the device;
   - a default gateway; and
   - a DNS server list.

5. A method for managing, at a device, a virtual private network (VPN) session between the device and a first VPN server, the method comprising:
   - establishing a VPN session between the device and the first VPN server;
storing one or more VPN parameters for the VPN session between the device and the first
VPN server on the device;
suspending the VPN session between the device and the first VPN server;
establishing a VPN session between the device and a second VPN server;
storing one or more VPN parameters for the VPN session between the device and the
second VPN server on the device;
suspending the VPN session between the device and the second VPN server; and
resuming the VPN session between the device and the first VPN server by retrieving said
one or more VPN parameters for the VPN session between the device and the first VPN server
from the device.

6. The method of claim 5, wherein said suspending the VPN session between the device and
the first VPN server includes preventing a user of the device from accessing the VPN session
between the device and the first VPN server without informing the first VPN server of such
prevention.

7. The method of claim 5, wherein said one or more VPN parameters includes a security
association.

8. The method of claim 7, wherein said one or more VPN parameters further includes at
least one parameter selected from the group consisting of:
a domain name service (DNS) server address;
an IP address of the device;
a default gateway; and
a DNS server list.

9. An apparatus for managing, at a device, a virtual private network (VPN) session between
the device and a VPN server, the apparatus comprising:
a VPN session establishe π
a VPN parameter storer coupled to said VPN session establishes
a VPN session suspender coupled to said VPN parameter storer;
a non-VPN session establisher;
a non-VPN session terminator coupled to said non-VPN session establisher; and
a VPN session resumer coupled to said VPN parameter storer and to said non-VPN session terminator.

10. An apparatus for managing, at a device, a virtual private network (VPN) session between the device and a first VPN server, the apparatus comprising:
a first VPN session establisher;
a first VPN parameter storer coupled to said first VPN session establisher;
a first VPN session suspender coupled to said first VPN parameter storer;
a second VPN session establisher;
a second VPN parameter storer coupled to said second VPN session establisher;
a second VPN session suspender coupled to said second VPN parameter storer; and
a first VPN session resumer coupled to said first VPN parameter storer and to said second VPN session suspender.

11. An apparatus for managing, at a device, a virtual private network (VPN) session between the device and a VPN server, the apparatus comprising:
means for establishing a VPN session between the device and the VPN server;
means for storing one or more VPN parameters for the VPN session on the device;
means for suspending the VPN session;
means for establishing a non-VPN session between the device and a non-VPN host;
means for terminating said non-VPN session;
means for resuming the VPN session by retrieving said one or more VPN parameters for the VPN session from the device,

12. The apparatus of claim 11, wherein said means for suspending includes means for preventing a user of the device from accessing the VPN session without informing the VPN server of such prevention.
13. The apparatus of claim 11, wherein said one or more VPN parameters includes a security association.

14. The apparatus of claim 13, wherein said one or more VPN parameters further includes at least one parameter selected from the group consisting of:
   - a domain name service (DNS) server address;
   - an IP address of the device;
   - a default gateway; and
   - a DNS server list.

15. An apparatus for managing, at a device, a virtual private network (VPN) session between the device and a first VPN server, the apparatus comprising:
   - means for establishing a VPN session between the device and the first VPN server;
   - means for storing one or more VPN parameters for the VPN session between the device and the first VPN server on the device;
   - means for suspending the VPN session between the device and the first VPN server;
   - means for establishing a VPN session between the device and a second VPN server;
   - means for storing one or more VPN parameters for the VPN session between the device and the second VPN server on the device;
   - means for suspending the VPN session between the device and the second VPN server; and
   - means for resuming the VPN session between the device and the first VPN server by retrieving said one or more VPN parameters for the VPN session between the device and the first VPN server from the device.

16. The apparatus of claim 15, wherein said means for suspending the VPN session between the device and the first VPN server includes means for preventing a user of the device from accessing the VPN session between the device and the first VPN server without informing the first VPN server of such prevention.
17. The apparatus of claim 15, wherein said one or more VPN parameters includes a security association.

18. The apparatus of claim 17, wherein said one or more VPN parameters further includes at least one parameter selected from the group consisting of:
   - a domain name service (DNS) server address;
   - an IP address of the device;
   - a default gateway; and
   - a DNS server list.

19. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for managing, at a device, a virtual private network (VPN) session between the device and a VPN server, the method comprising:
   - establishing a VPN session between the device and the VPN server;
   - storing one or more VPN parameters for the VPN session on the device;
   - suspending the VPN session;
   - establishing a non-VPN session between the device and a non-VPN host;
   - terminating said non-VPN session;
   - resuming the VPN session by retrieving said one or more VPN parameters for the VPN session from the device.

20. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for managing, at a device, a virtual private network (VPN) session between the device and a first VPN server, the method comprising:
   - establishing a VPN session between the device and the first VPN server;
   - storing one or more VPN parameters for the VPN session between the device and the first VPN server on the device;
   - suspending the VPN session between the device and the first VPN server;
establishing a VPN session between the device and a second VPN server;

storing one or more VPN parameters for the VPN session between the device and the second VPN server on the device;

suspending the VPN session between the device and the second VPN server; and

resuming the VPN session between the device and the first VPN server by retrieving said one or more VPN parameters for the VPN session between the device and the first VPN server from the device.
FIG. 2
4/7

Begin

Establish a VPN session between the device and the VPN server

Receive a request to access a non-VPN host from a user

Store one or more VPN parameters for the VPN session on the device

Suspend the VPN session

Establish a non-VPN session between the device and the non-VPN host

Terminate the non-VPN session

Resume the VPN session by retrieving the one or more VPN parameters for the VPN session from the device

End

FIG. 4
Begin

Establish a VPN session between the device and the first VPN server

Receive a request to access a second VPN from a user

Store one or more VPN parameters for the VPN session between the device and the first VPN server on the device

Suspend the VPN session between the device and the first VPN server

Establish a VPN session between the device and a second VPN server

Store one or more parameters for the VPN session between the device and the second VPN server on the device

Suspend the VPN session between the device and the second VPN server

Resume the VPN session between the device and the first VPN server by retrieving the one or more VPN parameters for the VPN session between the device and the first VPN session from the device

End

FIG. 5
FIG. 6
FIG. 7