

Device and method for routing secure communication streams between remote sites

5 The subject of the present invention is a device and a method for conveying, between remote sites, secure communication streams that are subject to broadcast constraints.

The invention concerns the field of network architectures, and notably networks requiring security provision for the streams interchanged between the various entities that compose them.

10 The invention more precisely concerns architectures composed of a plurality of remote local area networks, or LAN networks, interconnected by means of a plurality of wide area networks, or WAN networks, which are also called infrastructure networks. Each local area network may be connected to one or more wide area networks by one or more connecting links. Moreover,
15 the communication between local area networks must be secure.

In such an architecture, the local area networks constitute enclaves in the sense that the streams departing from each of these enclaves are secure. The enclaves are able to communicate among one another only by
20 means of a wide area network, for example an Internet public network managed by an access provider. A wide area network constitutes a transport network for the enclaves in the sense that it provides access to the communication medium and a transport service for the packets allowing connectivity between remote enclaves to be ensured.

25 Access, for a given local area network, to a plurality of redundant transport networks allows the reliability of communications to be increased. This multiplicity of the access to transport networks, whether a plurality of links to different WAN networks or a plurality of links to one and the same WAN network are involved, constitutes a technique that is commonly referred
30 to as "multihoming".

In a network architecture of this type, it is possible and desirable to implement a quality of service policy that allows a data stream that is to be transmitted to have the communication link that is best suited to its needs and constraints associated with it.

The invention can be applied notably to network architectures implementing the "multihoming" technique. The invention can be applied particularly to IP networks.

5 A general technical problem associated with networks of this type is the routing and conveyance of data streams between remote enclaves so as to observe the broadcast constraints associated with each of them.

10 This problem is all the more complex when the data communicated between two enclaves cannot be transmitted in plain form through the various transport networks for reasons of confidentiality, and the capability of the transport networks to satisfy such or such a constraint is unrecognized. The reason is that the information concerning the features of the communication links that an infrastructure network provides is not made available to the enclaves that said network serves.

15 In order to meet the confidentiality constraint, logical partitioning of the network is performed by introducing a device for ciphering the streams at the interconnection between each enclave LAN network and the WAN network(s). Reference is commonly made to the red part to denote the area of the network in which the data are manipulated in plain form and the decisions, notably routing and conveyance decisions, are taken. On the other hand, the black part denotes the area of the network in which the data are ciphered. The local area networks are situated in the red part of the network and the transport networks are situated in the black part of the network. The streams sent from a source enclave are thus ciphered by a ciphering device
20 before traveling through a transport network, and are then deciphered at the destination enclave.
25

A network architecture example to which the invention can be applied is shown in figure 1.

30 Two remote local area networks S1 and S2 are interconnected by means of two transport networks WAN_M and WAN_C. The users A1_S1,A2_S1 of the first local area network S1 communicate with the users B1_S2,B2_S2 of the second local area network S2. In order to partition the streams between the red R and black N parts of the network, a ciphering device Z_S1,Z_S2 is arranged between each local area network S1,S2 and
35 the transport networks to which it is connected. Routing devices

R1_S1,R1_S2 are situated near the local area networks, in the red part, so as to implement the path choice decisions allowing a stream transmitted from the first local area network S1 to be conveyed to the second local area network S2. In the black part, on the other side of the ciphering devices
5 Z_S1,Z_S2, routing devices R2_S1,R2_S2 are used in order to select the output associated with the transmission link chosen for transmitting the packets.

The example in figure 1 is limited to two enclaves that are directly connected by means of two transport networks, but the invention is not
10 limited to this example. More transport networks may be available. The connecting links between local area networks and transport networks may be of different types, for example ADSL link, satellite, or wireless link.

It is equally possible that two enclaves wishing to communicate are not directly connected, or that this direct connection does not meet or no
15 longer meets the imposed constraints. In this case, the communication between the two remote enclaves can be effected, under the expected conditions, only by passing through one or more intermediate enclaves.

A problem therefore exists for conveying the data streams between
20 remote enclaves, taking into account the quality of service constraints of the streams and the features of the transmission links, when the streams transmitted through the transport networks need to be ciphered or secured.

There is more than one known solution allowing implementation of
25 routing methods for networks such as described above.

Publication [1] concerns the techniques referred to as "multihoming". In this article, the authors demonstrate the benefits that the use of multiple connectivity means can bring in terms of performance. The problems surrounding the choice of output link for an enclave on the basis of various
30 performance criteria for the links and the features of the streams transmitted are introduced. The diversity of the links may be the result of a single operator or of several different operators. However, the choice of output link for a source enclave does not, on its own, allow implementation of a strategy of routing via an intermediate enclave in order to join an indirectly connected

destination enclave. This requires the ability to inspect not only the output link but also all the following ones, and thus to set up a complete path.

In publication [2], the authors propose mechanisms for setting up a logical network of "overlay" type and providing for nonciphered streams to be routed between the nodes that compose said network. The term "overlay" denotes a network topology constructed from logical links between the nodes of this network. A logical link corresponds to a possible access path between two nodes and is different than a physical transmission link between two nodes. In particular, a logical link may involve the aggregation of several contiguous physical links. The proposed routing mechanism allows the standard routing used in a network such as the Internet to be shorted in order to improve performance and to provide for better resilience in the event of a problem. However, such mechanisms require the nodes to communicate among one another in order to maintain the logical network and in order to interchange performance information on the logical links.

The two aforementioned references do not take into account the constraints linked to ciphering of the streams transmitted between remote enclaves and do not propose a mechanism allowing secure communications to be conveyed. The proposed routing methods cannot work for ciphered streams without a mechanism allowing control of the inspection plan for the black part in order to ensure that these communications are conveyed to the nodes of the logical network for which they are intended.

Moreover, reference [1] does not allow provision for conveyance between remote enclaves by passing through one or more intermediate enclaves.

The French patent application from the applicant filed under the number 1005089 is likewise known.

This application relates notably to a system for managing secure streams between two interconnected enclaves via a plurality of transport networks. The invention described allows a first solution to be provided for the problem of conveying ciphered streams but has certain limitations. It notably presupposes the implementation of complete networking between the enclaves that are capable of communicating. Therefore, the functionalities

proposed cannot be applied in the case where two enclaves, source and destination, are not directly interconnected by at least one transport network.

This scenario can appear for several reasons. Cost optimization may justify such choices of architecture, but this situation can also arise when one
5 or more existing link(s) do not (or no longer) allow the streams to be conveyed under the expected conditions, for example for problems pertaining to loss of connectivity, or deterioration of the quality of service features. The mechanisms proposed in this patent application therefore do not support any failure of the links that is caused by a breakdown of connectivity, a
10 configuration error or deterioration of the performance on an initially selected path.

The data transport mechanism MPLS (MultiProtocol Label Switching) based on the use of labels or tags for formulating conveyance decisions in a
15 communication network is likewise known. This mechanism is notably described in the document RFC5920 from the standardization committee IETF.

Figure 2 uses an example to illustrate a network architecture that is suited to use of the MPLS mechanism for conveying secure streams.

20 A plurality of enclave local area networks E1,E2,E3,E4 are interconnected by means of a plurality of transport networks WAN_1,WAN2. In order to ensure the confidentiality of the data streams conveyed through the transport networks, said data streams are ciphered on departing from an enclave local area network via a ciphering mechanism.

25 Each enclave local area network has a first routing device R1_E1,R1_E2,R1_E3,R1_E4 that is capable of formulating conveyance decisions for the streams from the enclave with which it is associated and bound for another enclave. The first routing device receives the data streams in plain form, said device being situated in the red logical part of the network.

30 Each enclave local area network is also associated with a second routing device, for each transport network to which it is connected. Thus, the enclave networks E2 and E3 are each linked to two routing devices R2_E2_W1, R2_E2_W2, R2_E3_W1,R2_E3_W2 that allow the ciphered streams to be switched through the transport networks WAN_1,WAN2.

The second routing devices receive the ciphered streams, said devices being situated in the black logical part of the network.

In a network such as that in figure 2, there is, for security reasons, a first routing plan for the routing devices in the red part of the network and a
 5 second routing plan for the routing devices in the black part of the network.

In order to provide security for the communications between the routing devices R1_E1,R1_E2,R1_E3,R1_E4 in the red logical part of the network, it is necessary to set up secure tunnels between each source device and each destination device, specifically through the various transport
 10 networks. The IPSec protocol, notably described in the standard from the IETF referenced under the number RFC 4301, is a means for setting up such secure tunnels. These secure tunnels can be set up only between two ends of a point-to-point link. In practice, the packets are ciphered in the red part of an enclave local area network and then the ciphered tunnel is based on the
 15 routing device in the black part and its counterpart connected to the destination enclave local area network.

Figure 3 illustrates the setup of secure tunnels for communication between the various enclave networks.

For the enclave networks E2,E3 that are linked to at least two different
 20 transport networks WAN_1,WAN_2, two secure tunnels need to be set up. The first secure tunnel T2_3_W1 is set up through the first transport network WAN_1 through the associated routing devices R2_E2_W1,R2_E3_W1 of the black logical part of the network. The second secure tunnel T2_3_W2 is
 25 set up through the second transport network WAN_2 through the associated routing devices R2_E2_W2,R2_E3_W2 of the black logical part of the network.

The routing plan of the black logical part of the network allows definition of the path taken by the packets transmitted through the secure
 30 tunnels. This routing plan allows the ciphered data packets to be conveyed between the routing devices of the red logical part that are associated with the source and destination enclaves.

Thus, the MPLS mechanism requires the use of ciphering tunnels for each transport network.

Moreover, when the path selected for conveying a secure stream from a source enclave to a destination enclave uses other intermediate enclaves, the use of the MPLS mechanism associated with a ciphering protocol requires the packets to be deciphered at each intermediate enclave because
5 the routing is formulated in the red part of the network.

By way of example, if a data stream 300 needs to be conveyed from the source enclave E1 to the destination enclave E4 by passing through the intermediate enclaves E2,E3, this stream travels through a plurality of successive secure tunnels between each pair of enclaves. At each
10 intermediate enclave, the stream is deciphered and put back up into the red part of the network in order to extract the information in plain form that is necessary for the routing.

The reason is that the routing devices of the red part of the network, which are transmitters of communication streams, take conveyance decisions
15 on the basis of the information contained in the packets before ciphering. They set up suitable conveyance in the red routing plan by means of the signaling 301 and send the packets through the chosen secure tunnel. The signaling stream 301 of the red routing plan and the communications are ciphered because they use secure tunnels. However, on account of the
20 isolation between the red and black routing plans, which isolation is imposed by the security provision for the streams, only the red routing plan is capable of processing the conveyance of these communications. A rebound to an intermediate enclave is therefore manifested by the packets going back up to the routing device of the red part, which, being one end of a secure tunnel,
25 decipheres the packets and conveys them to the next secure tunnel so that they are ciphered again.

The use of the MPLS mechanism associated with the use of secure tunnels therefore exhibits drawbacks because it requires numerous deciphering and ciphering operations within the intermediate enclaves. This
30 gives rise to implementation complexity problems but also confidentiality problems, because the secure streams are deciphered in an enclave that is neither the source enclave nor the destination enclave.

The aim of the present invention is to overcome the limitations of the
35 aforesaid solutions by proposing a mechanism for conveying ciphered

streams between remote enclaves that takes account of the situations in which all the enclaves are not directly linked by one or more transport networks.

5 The invention likewise addresses the situations in which there is a direct connection between two enclaves but in which this connection is not or no longer capable of satisfying the constraints associated with certain streams to be transmitted.

10 In these scenarios, it is necessary to set up a system that allows the traffic from a source enclave to be conveyed to a destination enclave by passing through one or more intermediate enclaves. Thus, through the implementation of traffic engineering mechanisms, the invention allows the ciphred streams to be conveyed by making the best use of all of the available network resources, and the quality of service required for streams defined as vital to be ensured in the event of the resources being inadequate
15 or partially unavailable.

The subject of the invention is a device for interconnection and routing between an enclave local area network and at least one transport network, characterized in that it comprises:

- 20 • first means that are suited to selecting, for a communication stream from said source local area network, at least one path to the enclave network for which it is intended and to associating this path with a marking value,
- means for inserting the marking value into a header field of the
25 packets in said stream,
- ciphering means for the entirety of said stream with the exception of said header fields,
- second means that are suited to receiving a ciphred stream transmitted by said first means or from another enclave local area
30 network and to switching it, without deciphering it, to the next node of the network situated on the selected path, on the basis of the marking value read from the header field of said packets,
- a gateway for communicating to said second means the
35 association between the marking value and the switching to be applied on the basis of the path selected by said first means.

In one variant embodiment of the invention, said first means are moreover suited to:

- setting up and maintaining at least one connectivity graph of the overall logical topology of the network containing all of the logical links connecting the enclave local area networks to one another and at least one piece of information relating to the transmission quality on said links,
- selecting the path for accessing the destination enclave network on the basis of said quality information and at least one conveyance constraint for said stream to be transmitted, so as to observe this constraint,
- communicating the selected path and the associated marking value to said first means of the other interconnection and routing devices situated on said path.

In one variant embodiment of the invention, said second means are moreover suited to modifying the value, which is associated with the selected path, of the header field of the packets received from a transport network.

In one variant embodiment of the invention, said first means are implemented by a first router, said second means are implemented by a second router, and the gateway is realized by a communication channel provided by the ciphering means.

In one variant embodiment of the invention, the networks are IP networks and the header field is the DSCP field of the IP packet.

In one variant embodiment of the invention, the ciphering means implement the IPsec protocol.

The subject of the invention is likewise a method for conveying a ciphered stream in a network having a plurality of enclave local area networks that are interconnected via at least one transport network, characterized in that it involves, for the purpose of conveying said ciphered stream from a source enclave network to a destination enclave network:

- setting up and maintaining at least one connectivity graph of the overall logical topology of said network containing all of the logical links connecting the enclave local area networks to one another and at least one piece of information relating to the transmission quality on said links,

- selecting, on the basis of said quality information and at least one conveyance constraint for said stream, at least one path for accessing the destination enclave network that allows this constraint to be observed,
- 5 • associating with the selected path, for each enclave network situated on said path, a marking value and communicating this association to the other enclave networks situated on said path,
- inserting this value into a header field of the packets in said stream,
- 10 • ciphering the entirety of said packets with the exception of said header field,
- for each enclave network receiving said ciphered packets, determining the next destination for said stream by reading the value of said header field and interpreting the associated path,
- 15 without deciphering said packets.

In one variant embodiment, the method according to the invention moreover involves reserving the available resources on said selected access path for the transmission of said stream.

- 20 In one variant embodiment, the method according to the invention moreover involves, for each enclave network receiving said packets, modifying the value of the header field of the packets with a marking value that is specific to said enclave network.

- 25 In one variant embodiment, said quality information comprises at least the passband or the delay or the jitter or the packet loss rate.

In one variant embodiment, said conveyance constraints comprise at least quality of service constraints, criticality of the service constraints, priority constraints or geographical constraints.

- 30 In one variant embodiment, an alternative path is selected as backup for the main path.

In one variant embodiment, the selection of said access path takes into account a scheduled interruption to the connectivity on at least one link provided by at least one transport network.

Other features and advantages of the invention will emerge on reading the description that is provided with regard to appended drawings, in which:

- figure 1 shows a first network architecture example, which network architecture is composed of enclaves interconnected by means of a plurality of transport networks,
- figure 2 shows a second network architecture example that is suited to the use of the known MPLS mechanism associated with the use of secure tunnels, for example secured via the IPSec protocol,
- figure 3 shows an illustration of the drawbacks of the MPLS mechanism,
- figure 4 shows a second network architecture example illustrating the problems surrounding conveying ciphered streams between two remote enclaves,
- figure 5 shows a functional overview of the device for routing ciphered streams according to the invention,
- figure 6 shows a network architecture example that is suited to the use of the device and the method for conveying secure streams according to the invention,
- figure 7 shows an illustration of the advantages of the invention, notably vis-à-vis the known MPLS mechanism associated with the use of secure tunnels.

Figure 4 uses a diagram to illustrate the problems surrounding conveying ciphered streams from one enclave to another in a network architecture such as that shown in figure 1.

A first enclave local area network E_201 is interconnected with two other enclave local area networks E_202, E_203 in the following manner. The first local area network E_201 is connected to the second local area network E_202 by means of a first transport network T_204. The first local area network E_201 is likewise connected to the third local area network E_203 by means of a second transport network T_205. The second and third local area networks E_202, E_203 are connected by means of a third transport network T_206.

In order to set up a connection from the first local area network E_201 to the third local area network E_203, the most direct path involves passing through the second transport network T_205. However, the connection provided by this transport network T_205 may be faulty, for example for reasons of loss of connectivity or limitation of the passband.

In this case, it is necessary to set up a system allowing the traffic from the first local area network E_201 to be conveyed to the third local area network E_203 by sending it through one or more intermediate enclaves.

In the example in figure 4, one possible logical path involves transmitting the traffic stream to the first transport network T_204 bound for the second local area network E_202, and then to the third transport network T_206 bound for the third local area network E_203.

Figure 4 moreover schematically shows the interconnection and routing devices D_211, D_212, D_213, situated between each local area network and each transport network or group of transport networks to which it is connected, which are necessary in order to separate the red part and the black part of the network and that aim, notably, to secure, by ciphering, the streams sent from each enclave and, respectively, by deciphering, the streams received by each enclave.

In a general manner, there is, in such a network, a need for a mechanism for conveying ciphered streams that allows selection and setup of the logical path that is most suited to the transmission of a data stream, on the basis of the constraints of the stream and the quality of service features that are provided by the various potential logical paths. The aim of the invention is to propose a solution that addresses this problem by adapting the interconnection and routing devices D_211, D_212, D_213 so that they implement a mechanism for conveying ciphered streams.

Figure 5 uses a functional overview to schematically show the device for conveying ciphered streams according to the invention.

Such a device D is positioned at the output of each network enclave, so as to provide for interconnection between an enclave E_S and the various transport networks T1,T2,T3 to which said enclave is connected, as shown in figure 4.

The device D according to the invention communicates with the enclave E_S in plain form, that is to say that the data streams transmitted between the device D and the enclave E_S are not secure. On the contrary, the communication between the device D and the transport networks
5 T1,T2,T3 is secure since the streams leaving or entering the device D and bound for or from the transport networks T1,T2,T3 are ciphered.

The device D is suited to implementing a routing mechanism that allows a stream from the enclave E_S and bound for a remote enclave E_D to be conveyed, under optimum quality of service conditions.

10

The device D comprises a first module 311 for formulating a conveyance decision for a stream f from the enclave E_S and bound for a remote enclave E_D. The first module 311 communicates directly with the enclave E_S and is situated in the red logical part of the network. The device
15 D likewise comprises an interface module 321 that is notably in charge of applying the conveyance decision by sending the stream from the enclave E_S on the communication link and the transport network T1,T2,T3 that have been chosen. This interface module 321 is situated in the black logical part of the network. A ciphering/deciphering device 331 is situated between the first
20 module 311, from which it receives or to which it transmits a data stream in plain form, and the interface module 321, from which it receives or to which it transmits an at least partially ciphered stream. By way of example, the ciphering device 331 implements the ciphering protocol IPSec. The implemented ciphering method is suited to ciphering the entirety of the
25 packet with the exception of at least one field of the header of the packet that is used to append a marking. A gateway 341 likewise links the red part (module 311) and the black part (module 321) of the device in order to provide for secure partitioning of the communications between the two parts while allowing the interface module 321 to be informed of the switching
30 choices determined by the first module 311.

The module 311 for formulating a conveyance decision is composed of a plurality of subfunctions that interact in order to associate with a stream f to be transmitted the logical path that is best for reaching its destination on
35 the basis of a plurality of constraints.

A first function 312 explores and supervises the logical links of the network in a neighborhood close to the enclave E_S and formulates quality information for each link that connects the enclave E_S to its neighboring
5 enclaves. Neighboring enclaves are understood to mean the local area networks situated a short distance from the enclave E_S, that is to say that are able to be reached from the enclave E_S by traveling through a single transport network.

The supervised links are logical point-to-point links between two local
10 area networks interconnected via a transport network. For example, the logical links are made up of tunnels between two local area networks. By way of example, the logical links are found by reading elements for configuring the enclave E_S. The tunnels existing within the network exist only if the two associated enclaves are authorized to set up a tunnel between them and are
15 configured to this end. A tunnel is considered to be a logical link, or a link called an "overlay", insofar as the underlying physical links and equipment traveled through in order to reach the end of a tunnel are set aside.

The supervision can be realized on the basis of two approaches. Passive supervision involves formulating quality information on the basis of
20 the useful traffic sent or received on each supervised communication link. Active supervision involves probing the network by generating probe traffic dedicated to this supervision between neighboring enclaves. These generated exchanges allow quality information to be determined on the communication links. The quality information notably includes the available
25 passband on a link, the transmission delay, the jitter or else the packet loss rate on this link.

A second function 313 provides for the broadcast of the topology and quality information from the logical links so as to inform each enclave local
30 area network of the logical topology of the network in its entirety and of the features associated with each link.

To this end, the information interchange function 313 transmits the features of the logical links that are known to it to the neighboring enclaves, that is to say those that are directly connected to the present enclave through
35 a logical link.

Moreover, the function 313 receives equivalent information from the neighboring enclaves. In this way, each device D associated with each enclave can reconstruct, from the information received from its neighboring enclaves after successive iterations, the overall topology of the logical
5 network with the quality features that are associated with each link.

The interchanges between the functions 313 of each device D in the network take place at regular intervals of time so that the knowledge of the information characterizing each link continues to be up to date for each enclave.

10 The following nonlimiting example allows the role of the function 313 to be illustrated.

An enclave A is connected to an enclave B through a logical link enjoying a passband of 20 Mbits/s. The enclave B is itself connected to an enclave C through a link for which the available passband is equal to
15 30 Mbits/s. On the basis of the information collected by the supervision function 312, a message containing the connectivity and topology information is generated by the function 313 and sent to the other ends of the links. A message is thus transmitted from the enclave A to the enclave B, from the enclave B to the enclaves A and C and from the enclave C to the enclave B.
20 Once this step has ended, the enclave B has complete knowledge of the overall topology of the network formed by the enclaves A, B and C. A second step is necessary in order to communicate the information acquired by the enclave B to the enclaves A and C.

Alternatively, the broadcast of the topology information can be
25 implemented through the use of one or more enclave(s) dedicated to the relay function in order to communicate the information to all the enclaves. When a plurality of relay enclaves are used, each relay enclave communicates the topology information only to the enclaves that are dependent on said relay enclave. When this alternative is used, the
30 information interchanges provided by the function 313 are no longer performed between neighboring enclaves, step by step, but by means of a relay enclave that then retransmits the aggregated information to the enclaves for which it is responsible.

Any other method allowing provision for the interchange and broadcast of topology information between remote enclaves in the network is compatible with the invention.

5 The subfunctions 312 and 313 of the module 311 thus allow a complete and up-to-date view of the logical topology of the network to be constructed and maintained in the red part of each enclave. This topology is realized by a connectivity graph of all of the available resources within the network and is stored in a database 314.

10 In one variant embodiment of the invention, a plurality of graphs may be stored and maintained, each representing the optimum solution according to one or more particular criteria.

 When a stream to be transmitted from the enclave E_S appears, the
15 packets arrive in the module 311 and first of all travel through the marking module 317. The function of this module is to associate a marking value X with all the packets in this stream, to append this marking in the header of each packet and to transmit a copy of the packets to a function 315 analyzing and formulating a conveyance decision. In the case of an IP technology, the
20 header field used to append the marking X may be the DSCP (Differentiated Services Code Point) field of the IP header. This field is coded over 6 bits, and it is the only part of the IP header that continues to be able to be read after ciphering. Thus, this marking is an indicator that constitutes the only means of recognizing, in the black part, the packets that belong to a stream
25 when they are ciphered. As for the original packets, these are transferred to the ciphering device 331.

 The ciphering operation performed by the function 331 involves ciphering the entirety of the data in the transmitted packets with the exception of at least the aforesaid header field.

30

 On the basis of the graph(s) stored in the database 314, the decision function 315 analyzes the copy of the packets and selects the optimum path for conveying a stream f to a destination enclave on the basis of the features of the logical links of the network and the conveyance constraints for the
35 stream.

These constraints notably relate to the quality of service associated with the stream, that is to say the speed required for transmitting the stream, the tolerable conveyance delay, the jitter or else the acceptable loss rate.

The conveyance constraints may likewise relate to the criticality of the service associated with the stream to be transmitted and to the conveyance priority to be allocated to this stream. Geographical constraints may likewise exist, for example translating into a ban on sending through a given transport network. Finally, constraints pertaining to the cost of accessing the transport networks, which are potentially different, may likewise come into play in the decision-making performed by the function 315.

Two scenarios arise when formulating a decision relating to the conveyance of a stream that is to be transmitted.

If a direct path satisfying the constraints for conveying the stream exists between the source enclave and the destination enclave, this path is chosen. This scenario does not require any signaling prior to the stream being conveyed.

The gateway 341 allows communication between the red and black parts in order to inform the switching module 342 of the correspondence between the marking in the header field and the output of the device D that needs to be used. Various outputs of the device D correspond to the various communication links, each being potentially linked to various transport networks.

Thus, when the switching module 342 receives a data packet to be transmitted, it provides for the packet to be switched to the output previously associated with the value read from the header field of the packet, in accordance with the conveyance decision. The switching module 342 is situated in the black part of the network and therefore has no knowledge of the data in the packet that are ciphered, nor of the final destination of the packet, nor even of the path that will be taken in order to convey this packet to its destination. Thus, secure partitioning of the interchanges between the black part and the red part is performed. Only the header field associated with the selected path is not ciphered during the ciphering step, which allows the packet to be conveyed to its destination without requiring access to the ciphered information that the packet contains.

In the case in which there is not a direct path between the source and destination enclaves, or if one exists but it does not satisfy the conveyance constraints for the stream, the conveyance decision ends up by selecting another logical path, which requires the stream to be sent through one or
5 more intermediate enclaves. The intermediate enclaves traveled through must then be configured so that the chosen conveyance is effectively implemented for the stream under consideration.

The role of the function 316 is to generate and communicate the
10 signaling messages prior to the transmission of a communication stream requiring conveyance through an intermediate enclave. A plurality of variant embodiments of this signaling function 316 are possible.

In a first embodiment, the selection of the whole path, composed of a succession of logical links and intermediate enclaves, is performed by the
15 subfunction 315 of the device D associated with the source enclave, which is the sender of the stream f to be transmitted.

The information relating to the selected path is associated with the marking value X previously appended by the module 317.

In the same way as when a direct path is selected, the switching module 342
20 of the device associated with the source enclave is configured so that the packets of the stream f to be transmitted are sent on the link that allows the first intermediate enclave to be reached. A signaling message is then generated and contains the information necessary for identifying the complete path, and also the information concerning the quality required for
25 the stream and the associated marking value X.

The signaling message is transmitted to the first intermediate enclave on the selected path, that is to say the enclave that neighbors the source enclave, so as to communicate thereto the information associated with the marking value X of the header field of the packets that compose the stream f
30 to be transmitted. On reception of this signaling message, the signaling function 316 of this first intermediate enclave (red part) peruses the path to be associated with the value of the header field and updates a table of correspondence, then configures the switching module 342 to indicate the conveyance action to be performed for the packets marked with this value X
35 that come from the source enclave.

This operation is then repeated step by step for each intermediate enclave situated on the selected path. Besides the implementation of the conveyance of the ciphered streams, this signaling can likewise allow the resources necessary for this conveyance to be reserved.

5

The packets of ciphered data in the stream *f* are then transmitted to the neighboring enclave that constitutes the first hop on the chosen path. To this end, these packets contain, in their header, the destination address of this first enclave.

10 With reference to the example in figure 4, the packets in the stream *f* are transmitted from the device D_211 to the device D_212 in a secure manner.

Owing to the signaling step performed beforehand, the switching subfunction 342 of the device D_212, which subfunction is situated in the
15 black part, is able to associate the value of the header field that has been read from the received ciphered packets with a particular path in the network. Thus, the device D_212 is able to convey the packets to their final destination, namely the enclave E_203, without the need to decipher them, and therefore without their reaching the red part of the device D_212. Thus,
20 an intermediate enclave is not capable of intercepting the streams that are not intended for it.

In one variant embodiment of the invention, the value *X* of the header field can be modified, during the signaling step, by the device *D* associated
25 with an intermediate enclave. This is because if, by way of example, this value *X* has already been associated with another operation, it can be modified to a new value *Y*. It is also possible to require the value of the field to be specific to each enclave. In this case, each device *D* associated with each intermediate enclave associates, for the same conveyance strategy, a
30 potentially different value of the header field that has a significance specific to the enclave.

When the transmitted stream is received by an intermediate enclave, it is the switching function 342 that modifies the value of the header field. The function 342, in the black part of the network, is able to perform this operation
35 of modifying the marking, of which it has been notified by the signaling

module during the step of configuring the black part. Thus, the action to be performed during the reception of packets having a given marking value X involves modifying the marking and conveyance on the next link constituting the logical path.

5

In another variant embodiment of the invention, the overall path allowing the stream f to be conveyed from the source enclave E_201 to the destination enclave E_203 is not decided by the device D associated with the source enclave E_201, but the decision module of each intermediate enclave
10 E_202 is asked, during the signaling phase, to decide, step by step, on the best logical link to be selected in order to continue conveying the packets to their final destination.

The conveying method according to the invention will now be
15 described, said method being implemented for the example in figure 4.

A communication stream f is sent from the network enclave E_201 to the network enclave E_203. The transport networks T_204, T_205, T_206 are situated in the black part of the network. Thus, the streams being sent through these various transport networks need to be secure so that access to
20 their content is rendered impossible.

The aim of the method according to the invention is to determine the optimum path that allows the secure stream f to be conveyed to the destination enclave by taking account of the features of the various links with regard to the constraints associated with this stream. It basically involves the
25 following steps executed by the interconnection and routing devices D_211, D_212, D_213 providing the interface between each enclave local area network and the black part of the network, which part is made up of the various communication links and transport networks.

The device D_211 associated with the source enclave E_201 explores
30 the network. It thus discovers that the enclave E_201 is connected to the enclave E_202 by means of the transport network T_204 and that the transport network T_205 connecting the enclaves E_201 and E_203 is faulty.

It communicates this information to the device D_212 associated with the enclave E_202 according to the mechanism associated with the function
35 312 described previously. The device D_212 in turn discovers that the

enclave E_202 is linked to the enclave E_203 by means of the transport network T_206.

Step by step and by successive iterations, all the devices D_211,D_212,D_213 discover or maintain their knowledge of the topology of the network and of the features of each communication link. This topology is stored and maintained in the form of one or more connectivity graphs in a database 314.

Alternatively, the topology information from the network is communicated by means of one or more enclaves that receive all of the information so as then to broadcast it to all of the remote enclaves in an aggregated manner.

The device D_211 then chooses the best path that allows the stream f to be conveyed from the source enclave E_201 to the destination enclave E_203. Taking into account the fault in the transport network T_205 that provides for a direct link between these two enclaves, the device D_211 selects the indirect path passing through the device D_212 in the enclave E_202.

A signaling phase is then started.

A signaling message is generated that contains the information allowing identification of the selected path, the transmission features thereof (passband, delay, jitter, error rate) and the marking value X associated with this path. This message is transmitted, hop by hop, to the enclaves situated on the selected path. On receiving the signaling message, each routing device D_212 updates a table of correspondence between the marking values and the associated path, and configures the switching module 342 situated in the black part in order to perform suitable conveyance.

In one variant embodiment, the marking value X of the packets is specific to each enclave.

Once the signaling phase has ended, all the enclaves situated on the selected path know what conveyance operation to perform on receiving a ciphered packet for which the value of the header field, for example the DSCP field, corresponds to an identified value in the table of correspondence. Each interconnection and routing device D_212 then conveys the received ciphered packet, on the basis of this header field value, to the next enclave on the path identified by virtue of this value, and so on

until the packet arrives at its destination. This operation is performed by the module 321 of the device D_212 situated in the black part of the network, so as to convey the packets without performing any deciphering. When the device D_213 receives the packet, the corresponding module 321 knows, on account of the absence of correspondence between the marking value and a conveyance action, that said packet has arrived at its destination, and can therefore transmit it to the module 331 for deciphering, and then to the routing module 317, which completes the conveyance of the packet to the destination in the enclave E_203.

In one variant embodiment, the overall path connecting the source enclave to the destination enclave is not determined totally by the routing device associated with the source enclave but rather is determined step by step by each of the routing devices associated with each enclave in the network.

The device according to the invention can be implemented in a single piece of equipment enjoying sizeable resources, or may have a first routing device 311 that is suited to implementing the processing operations in the red part of the network, a second routing device 321 that is suited to implementing the processing operations in the black part of the network, and a ciphering means 331 that provides for the link between the two. The gateway 341 may be provided by a communication channel implemented by the ciphering device and dedicated to this end.

Figure 6 illustrates the use of the device according to the invention that is described in figure 5 for application thereof to the architecture network already described in figure 2.

An interconnection and routing device D_601,D_602,D_603,D_604 is positioned at the output of each enclave network E1,E2,E3,E4 whatever the number of transport networks WAN_1,WAN_2 to which it is linked.

As indicated above, the device according to the invention may be implemented via a first routing device 311 situated in the red part of the network and a second routing device 321 situated in the black part of the network and having access only to the ciphered streams. By way of example, the ciphering 331 is performed using the IPSec protocol in tunnel mode and a gateway 341 allows communication between the red part and the black part

of the network so as notably to transmit the information that is necessary for matching the marker X of the header of the packets to the conveyance rules that need to be applied by the routing devices 321 of the black part. In other words, this gateway 341 authorizes the passage of conveyance instructions
5 from the red routing plan to the black routing plan. The implementation of such a gateway makes it possible to guarantee the confidentiality of the secure communications even when they are sent through an intermediate enclave network. On the other hand, owing to the invention, the number of secure tunnels to set up is decreased in relation to the use of the MPLS
10 mechanism described in figure 2. The reason is that the present invention requires, in the black part of the network, only a single routing device 321 per enclave network rather than one routing device per enclave network and per transport network.

15 Figure 7 illustrates the way in which the invention works and the differences therein using the MPLS mechanism combined with the use of the IPSec protocol for performing the ciphering.

A single secure tunnel exists between each pair of source and destination enclave networks. In particular, the enclaves E2 and E3
20 connected to two transport networks WAN_1, WAN2 require only a single IPSec tunnel because the device according to the invention allows the communication, in the black part of the network, of information concerning the conveyance of the ciphered stream without having to decipher the received packets by going back up to the red part of the network.

25 In the example in figure 7, in order to convey a secure data stream from the source enclave E1 to the destination enclave E4 by passing through the intermediate enclaves E2, E3, the routing device 311 of the red part of the network takes the conveyance decision on the basis of the information contained in the packets before ciphering. It sets up the suitable conveyance
30 in the red routing plan by means of signaling 701 that always uses the secure tunnels by going back up to the red part of each interconnection device according to the invention. The signaling traffic from the routing plan of the red part therefore remains secure. In each enclave sought by the secure stream, the gateway 341 of the interconnection and routing device according
35 to the invention allows the communication 703 of conveying instructions from

the red routing plan to the black routing plan. The ciphered data packets are, on the basis of these instructions, switched to the next intermediate enclave or to the destination enclave, while being maintained in the black part of the network, that is to say without deciphering the transmitted data at any moment. The control of the black routing plan by the red routing plan owing to the gateways 341 thus avoids the operations of deciphering, routing and ciphering of the packets at each intermediate enclave. The communications 702 remain secure since they use just a single ciphering tunnel that connects the source enclave to the destination enclave. In the example in figure 7, the secure stream from the enclave E1 and bound for the enclave E4 is sent via the secure tunnel 331, which has been set up via the IPSec protocol, for example. This secure tunnel passes through each routing device in the black part of the network situated on the selected path. The conveyance is effected hop by hop by virtue of the information communicated via the secure gateways 341.

Owing to the invention, secure streams initially conveyed between two directly connected enclaves can be redirected via intermediate enclaves when a problem arises on a direct link. The events capable of triggering this redirection mechanism may be losses of connectivity in the operator network that provides for this direct link, but also deteriorations in performance, these events being detected by virtue of the supervision module 312 of the device according to the invention.

The invention has the advantage of allowing secure streams to be conveyed between two remote enclaves by passing through one or more intermediate enclaves without the need to decipher them as they are sent through. The mechanisms implemented by the invention, particularly the partitioning between the red and black parts of the interconnection and routing device according to the invention, allow an optimum conveying strategy to be provided while retaining a large degree of security provision for the stream as it is sent through the various entities situated on its path.

When redirection takes place, the resources required for conveying all of the redirected streams are not necessarily available. In this case, a

preemptive function allows just part of the traffic to be conveyed, giving priority to streams that have a high level of criticality.

5 The invention likewise allows a protection and restoration mechanism to be implemented. When a path is selected, it is possible to provide and set up an alternative backup path on which streams, in particular critical streams, can be instantaneously redirected in the event of a problem on the initially used path.

10 Furthermore, in the event of a foreseeable interruption to the connectivity provided by a transport network, for example for maintenance reasons, the invention allows a mechanism of "Make before Break" type to be implemented, which involves setting up another path and redirecting the streams onto this path even before the interruption takes place.

15 The invention can be applied to any infrastructure network that requires a high level of security provision and resilience.

References

[1] A. Akella et al., "On The Performance Benefits of Multihoming Route Control", IEEE/ACM Transactions on Networking, vol. 16 (1), 2008, p. 91-104.

5

[2] D. G. Andersen et al., "Resilient Overlay Networks", in Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), 2001, p. 131-145.

CLAIMS

1. A device (D) for interconnection and routing between an enclave local
5 area network (E_201) and at least one transport network
(T_204,T_205,T_206), characterized in that it comprises:
- first means (311) that are suited to selecting, for a communication
stream from said source local area network (E_201), at least one
10 path to the enclave network (E_203) for which it is intended and to
associating this path with a marking value (X),
 - means (317) for inserting the marking value (X) into a header field
of the packets in said stream,
 - ciphering means (331) for the entirety of said stream with the
exception of said header fields,
 - 15 • second means (321) that are suited to receiving a ciphered stream
transmitted by said first means (311) or from another enclave local
area network (E_201,E_202) and to switching it, without
deciphering it, to the next node of the network situated on the
selected path, on the basis of the marking value (X) read from the
20 header field of said packets,
 - a gateway (341) for communicating to said second means (321)
the association between the marking value (X) and the switching to
be applied on the basis of the path selected by said first means
(311).
- 25
2. The device (D) as claimed in claim 1, characterized in that said first
means (311) are moreover suited to:
- setting up and maintaining (312,313) at least one connectivity
graph (314) of the overall logical topology of the network containing
30 all of the logical links connecting the enclave local area networks to
one another and at least one piece of information relating to the
transmission quality on said links,
 - selecting (315) the path for accessing the destination enclave
network (E_203) on the basis of said quality information and at

least one conveyance constraint for said stream to be transmitted,
so as to observe this constraint,

- communicating (316) the selected path and the associated marking value (X) to said first means (311) of the other interconnection and routing devices situated on said path.

5

3. The device (D) as claimed in either of the preceding claims, characterized in that said second means (342) are moreover suited to modifying the value, which is associated with the selected path, of the header field of the packets received from a transport network.

10

4. The device (D) as claimed in one of the preceding claims, characterized in that said first means (311) are implemented by a first router, said second means (321) are implemented by a second router, and the gateway (341) is realized by a communication channel provided by the ciphering means (331).

15

5. The device (D) as claimed in one of the preceding claims, characterized in that the networks are IP networks and the header field is the DSCP field of the IP packet.

20

6. The device (D) as claimed in claim 5, characterized in that the ciphering means (331) implement the IPSec protocol.

25 7. A method for conveying a ciphered stream (f) in a network having a plurality of enclave local area networks (E_201, E_202, E_203) that are interconnected via at least one transport network (T_204,T_205,T_206), characterized in that it involves, for the purpose of conveying said ciphered stream from a source enclave network (E_201) to a destination enclave network (E_203):

30

- setting up and maintaining (312,313) at least one connectivity graph (314) of the overall logical topology of said network containing all of the logical links connecting the enclave local area networks to one another and at least one piece of information relating to the transmission quality on said links,

35

- selecting (315), on the basis of said quality information and at least one conveyance constraint for said stream (f), at least one path for accessing the destination enclave network (E_203) that allows this constraint to be observed,
 - 5 • associating with the selected path, for each enclave network situated on said path, a marking value (X) and communicating (316) this association to the other enclave networks situated on said path,
 - inserting this value (X) into a header field of the packets in said stream (f),
 - 10 • ciphering (331) the entirety of said packets with the exception of said header field,
 - for each enclave network receiving said ciphered packets, determining the next destination for said stream (f) by reading the value of said header field and interpreting the associated path,
 - 15 without deciphering said packets.
8. The conveying method as claimed in claim 7, characterized in that it moreover involves reserving the available resources on said selected access path for the transmission of said stream.
- 20
9. The conveying method as claimed in either of claims 7 and 8, characterized in that it moreover involves, for each enclave network receiving said packets, modifying the value of the header field of the packets with a marking value (Y) that is specific to said enclave network.
- 25
10. The conveying method as claimed in one of claims 7 to 9, characterized in that said quality information comprises at least the passband or the delay or the jitter or the packet loss rate.
- 30
11. The conveying method as claimed in one of claims 7 to 10, characterized in that said conveyance constraints comprise at least quality of service constraints, criticality of the service constraints, priority constraints or geographical constraints.
- 35

12. The conveying method as claimed in one of claims 7 to 11, characterized in that an alternative path is selected (315) as backup for the main path.
13. The conveying method as claimed in one of claims 7 to 12, characterized in that the selection (315) of said access path takes into account a scheduled interruption to the connectivity on at least one link provided by at least one transport network.