

**System and method for managing secure flows between a
plurality of remote sites**

The present invention relates to a system and a method
5 for managing secure flows between a plurality of remote
sites, local or metropolitan area networks.

The invention relates to the field of the
telecommunication architectures of the networks and
10 notably the networks that have strong constraints in
terms of security. Such architectures may comprise both
sensitive private networks interconnected with non-
sensitive public networks. The sensitive networks have
strong resilience capabilities for routing the
15 sensitive flows for the benefit of the users. The non-
sensitive public networks handle the routing of the
non-sensitive flows for the benefit of other users. The
expression "sensitive flows" should be understood to
mean both the flows of a confidential nature and
20 routing constraints or constraints of an operational
nature. The protection confidentiality-wise of the
flows is handled by the applications or by other means
implemented in the serving networks (campus) and which
do not have a direct influence on the architecture of
25 the system.

Transport in the serving networks (that is to say LANs,
"Local Area Networks", and/or MANs, "Metropolitan Area
Networks") of the sensitive and non-sensitive flows is
30 characterized by the fact that all of the flows are
conveyed over a single non-sensitive MAN network (the
non-sensitive flows are by nature more voluminous and
affect a larger number of users). To handle the routing
protection, on wide area networks WAN, for all of the
35 flows (sensitive and non-sensitive), the latter are
transported encrypted over said networks WAN via IPsec
("Internet Protocol Security") tunnels.

The means with strong resilience capabilities are terrestrial infrastructure means with great resource capability or satellite infrastructure means with
5 smaller resource capability and having quality of service (QoS) constraints, for example in terms of latency times, transit times, packet loss.

Communication between the users situated in the serving
10 networks is constrained by the use of IPsec encryptors and it obeys communication rules that are generally established statically, these rules define the parties eligible to communicate (generally subnetworks) and the remote sites (the IPsec security equipment elements)
15 that these eligible parties can reach. Such information is contained in a database called SPD ("Security Policy Database"). The SPD base is not dynamically modifiable and requires manual configuration operations on the part of an operator. The set of rules entered in the
20 SPD base is called the "flow security policy".

The flows circulating between two remote local area networks are of different natures, they are identified by a traffic class, for example using the DiffServ
25 classification mechanism, the DiffServ field being a field of the header of an IP packet. The network edge equipment elements do not perform any processing on the flows according to traffic class, but in relation to a class of service, a class of service being a
30 combination of a set of traffic classes. This principle makes it possible to apply egalitarian processing to the flows that have identical technical constraints such as transit time for example.

35 With the current systems, the encryption is performed before the routing. It is necessary to have two routing plans, a routing plan in the red part of the network

(before the encryptors) and a routing plan in the black part of the network (after the encryptors). On the other hand, it is not possible to make a correlation between these two routing plans, because the black
5 routing plan is masked and inaccessible because of the use of VPN IPsec ("Virtual Private Network Internet Protocol Security") virtual private networks.

One known technique is to use two wide area networks
10 WAN in a "backup" function, that is to say that the second WAN network will be used only if the first has a connectivity failure. In the other cases and notably in the case of saturation of the WAN network, the flows continue to take the saturated WAN network.

15 Finally, to allow for simultaneous use of the two WAN networks, it is necessary to re-establish a routing topology on the basis of the red routing plan; this solution uses tunneling of the flows by the use of GRE
20 tunnels which make it possible to re-establish connectivity between the red router equipment elements and to create the red routing plan by the use of a link state protocol such as the IGP protocol (OSPF for example).

25 The prior art requires the implementation of a plurality of distinct products (switch, firewall, router and encryptor). The management and security operations are distinct and require a correlation
30 between the operators to define the establishment of the security policies and routing policies (GRE tunnels). Operation is made complex on the large networks since it is necessary to set up GRE tunnels between all the sites.

35 The implementation of a flow management policy is very limited by the simple fact that there is a limited

visibility of the content of the packets (DSCP field) and not of the origin and the destination of the flows, which implies taking routing decisions upstream (red plan).

5

The offset generated by the IPsec tunnels does not make it possible to ensure a coherent SLA between the MAN (users) and WAN (transit) networks, which is why it is necessary to have a router (in some cases called QoS
10 router) between the WANs and the encryptors whose main objective is to ensure consistency between the flows from the WAN and intended for the MANs, and vice versa.

A number of problems remain unresolved by the systems
15 of the prior art. Notably, the variable elongation of the size of the packets (overhead) imparted by the encryptor does not make it possible to have consistency on the QoS. The flow management policy is not carried out according to the type of operational flow. There is
20 no policy for distribution of the flows between the WANs. There is no reservation and preemption of the resources on the WANs which implement protocols such as RSVP.

25 The network edge equipment elements incorporate functionalities for managing classes of services through the use of a plurality of queues and they associate with these queues a particular process which guarantees the users of these services appropriate
30 processing of their flows in the event of congestion in the networks. These QoS principles and the associated rules are called "the flow processing policy".

Figure 1 presents an architecture of networks
35 interconnected with one another. One objective of such an architecture is to handle the secure setting up of one or more communication links between a first local

area network S1, also called network enclave, and a second local area network S2. These two remote network enclaves are interconnected by means of one or more public WAN_C or private WAN_M wide area networks, in
5 wired or satellite form. The flows transmitted between the two local area networks S1, S2 are encrypted, respectively decrypted, by an encryption device Z_S1, Z_S2 arranged between each local area network and the wide area network(s). One or more red routers R1_S1,
10 R2_S2 handle the switching of the flows intended for and from the network enclaves S1, S2. One or more black routers R2_S1, R2_S2 handle the switching of the encrypted flows through the wide area network(s) to the remote network enclave.

15

A first problem linked to this type of architecture relates to the partitioning between the wide area networks WAN on the one hand and the local area networks on the other hand because of the encryption of
20 the data flows. Only the data flows from one network enclave can reach another network enclave in conformity with the content of the SPD database. In other words, no data flow can circulate between a network enclave S1, S2 and a wide area network WAN. The communications
25 that are allowed are necessarily between two encryption equipment elements. This absence of the possibility of direct communication between a local area network and a wide area network poses a problem when wanting to determine the type of wide area network to be used to
30 set up a communication link on the basis of the intrinsic characteristics of a data flow from a network enclave. In practice, the flows transmitted can be ranked according to a quality of service which is assigned to them for example in relation to their
35 degree of priority (vital flow or not), to their bandwidth and bit rate requirements or even to the delay, jitter and/or packet loss constraints that they

can support. To be able to determine the communication channel, out of the available wide area networks WAN, that is best suited to the data flows to be transmitted, it is therefore necessary to set up a communication between the network enclave and the wide area networks in order to communicate the identified requirements. This type of communication is not possible with the known architectures because of the presence of the encryption equipment elements.

10

A second problem linked to the known secure architectures relates to the routing of data flows through the different wide area networks. The current routing protocols, for example the OSPF protocol, make it possible to route the flows according to the cost of the links. However, to be able to use a link state routing protocol between the remote local area networks S1, S2, it is necessary to set up direct links between these networks making it possible to circumvent the presence of the encryption equipment elements. Such a direct link is, for example, implemented using the GRE (Generic Routing Encapsulation) protocol. The routing protocols implemented in the wide area networks WAN have no interaction with the link state routing protocol implemented by the routers R1_S1, R1_S2; in fact they are masked by the IPsec tunnels. Also, the incidents which occur in the different WAN networks will be taken into account on the routers R1_S1, R1_S2 only on detection by the link state protocol of a malfunction. The malfunction observed by the router to change the routing is a break in the link, that is to say a break in the GRE tunnel. In this case, the link state protocol can route the flows to another WAN network. The loadsharing between the different WAN networks can be done provided that the link costs are identical.

35

This type of operation does not make it possible to route the flows intelligently by taking account of criteria on both of the wide area networks WAN. Nor does it make it possible to optimize the transit capacity of the WAN networks. This amounts to using only the WAN networks within their transit capacity or to provisioning excess resource on one or other of the WAN networks.

10 A third problem of the known secure architectures relates to the switching of the flows to the different available WAN networks according to the sensitivity of their content. In practice, the sensitive flows have to be directed to a secure private wide area network
15 whereas the non-sensitive flows can be directed to a public wide area network. To perform this switching, it is necessary to analyze the applications which are above the IP layer or to make use of a precise identification of the source and the destination of the
20 flows. The sites host users having administrative or operational functions, and these users are considered either to be vital users (in limited numbers) or non-vital users and they generate sensitive and non-sensitive flows. There is no correlation between the
25 vital users and sensitive flows; a non-vital user can generate sensitive flows.

The flows from local area networks LAN and/or MAN are encrypted for reasons of level of security of these
30 flows. In this case, the analysis of the packets can be performed only on the DSCP ("Differentiated Services Code Point") field of the IP packet, which benefits from a full unaltered copy on the part of the encryption equipment elements. Also, the switching of
35 the flows to one or other of the WAN networks can be performed only on the basis of this DSCP field which is limiting when it comes to performing a precise analysis

of the sensitivity of the flows.

The abovementioned three problems are directly or indirectly linked to the technical constraints introduced by the presence of encryption equipment elements which limit the possible exchanges between the black part (local area networks) and the red part (wide area networks) of the network.

Figure 2 illustrates a topology, similar to that of figure 1, of secure network architecture according to the prior art.

Such an architecture comprises users of the service area of a first local area network S1, which are respectively the subscribers A1_S1 and subscribers A2_S2. These users have different IP addresses, identifiable by their prefix. The users of the site S2 also have different addresses between subscribers B1_S2 and B2_S2 and with regard to the local area network S1. The flows between the users of the enclaved local area networks S1 and S2 are switched to the output routers R1_S1, R1_S2, or red routers, of each local area network. The routers R1_S1 and R1_S2 are optional. They make it possible, for example, to manage the subscribers of the network enclaves in the form of a plurality of communities having different attributes. They also make it possible to manage the available theoretical bandwidth by assigning priorities to the subscribers.

The system of figure 2 also comprises encryptors Z_S1, Z_S2. The encryptor Z_S1 ensures protection of the flows from the router R1_S1 intended for the router R2_S1. The protection is, for example, implemented using the IPSec protocol in tunnel mode. The security policy assigned to each encryptor makes it possible to

partition the flows from the local area network S1 and intended for users of the local area network S2. The IPSec encapsulation makes it possible to mask the addresses of the local area networks S1 and S2 from the
5 wide area networks WAN_C and WAN_M. The encryptor Z_S2 handles a role equivalent to the encryptor Z_S1 for the local area network S2. The IP addresses on the black interface of the encryptors are the only addresses visible to the wide area networks WAN_M and WAN_C. It
10 is these addresses which are used by these WAN networks to route the flows from and intended for the routers R2_S1 and R2_S2.

The black routers R2_S1, R2_S2 are situated between the
15 encryption devices Z_S1, Z_S2 and the wide area networks. They make it possible to switch flows to the wide area networks according to their flow processing policy. Such a policy consists, for example, in switching the sensitive flows to the private network
20 WAN_M and the non-sensitive flows to the public network WAN_C. Moreover, the black routers R2_S1, R2_S2 adjust the value of the DSCP field of the packets according to the classes of service offered by the wide area networks WAN. They also handle the formatting of the
25 packets to compensate for the redundancy introduced by the encryptors.

The private wide area network WAN_M conveys the flows between the local area networks S1 and S2 according to
30 a routing which is specific to it. The public wide area network WAN_C carries out the same routing functions according to its own parameters (topology, routing protocols, QoS, etc.). In the exemplary architecture of figure 2, the system comprises only two wide area
35 networks WAN_M, WAN_C, but it could apply equally to a greater number of wide area networks. The wide area networks WAN_M and WAN_C are transport service

providers which offer the following functionalities:

- Real time "Reporting" on the state of the links set up by the service provider. If, for example, following bad weather, there were to be congestion on the network WAN_C, the flows would continue to be switched thereto whereas they could have been routed, at least for the most vital among them, to the network WAN_M. The "Reporting" makes it possible to implement this type of switching policy.
- "Pre-emption & Priority Management": The internal problems in a WAN are reflected in the vast majority of cases in a reduction of the equivalent bandwidth and very rarely in a clean break in transmission. The remaining bandwidth must therefore be managed as best it can. This functionality allows strict priority management, at the flow level and not the packet level, and offer pre-emption mechanisms that make it possible to assign the remaining bandwidth to the most vital flows.
- "Protection and Restoration (P&R)": Some applications require there to be no interruption to the transport of the flows or, more precisely, for the interruptions to remain less than 50 ms. Moreover, this requirement is totally independent of the criticality of the application (vital or non-vital). The P&R makes it possible to express to the WAN_C or WAN_M the desire for a "back-up" path of 1 for 1, 1 for N or even P for N type. It is also possible to implement this type of mechanism at the "overlay" level. In other words, the nominal paths can be set up on one WAN and the "back-up" paths on the other WAN.
- "Make before Break": This functionality proves

interesting when maintenance operations have to be conducted on a WAN and the latter have an impact on the continuity of the established links. It is a case here of "preventing rather than curing". New routes
5 are computed and implemented before interrupting those which were in place. This type of mechanism can also be relayed at the "overlay" level. Instead of finding an alternative routing within one and the same WAN, the second WAN contributes.

10

The network architectures according to figure 2 make it possible to partially solve the third problem described above regarding the switching of the encrypted flows. In practice, it is possible to put in place a routing
15 policy based on the pairing of destination IP address and DSCP field value. The encryptor masks the source and destination IP addresses of the subscribers but, for obvious routing reasons, adds in clear source and destination IP addresses corresponding to the sending
20 and receiving encryptors. In other words, it involves creating a new network layer level header. In this new header, the value of the DSCP field corresponds to that presented at the input.

25 However, this solution is very inadequate when it comes to operating sophisticated switching policies. In practice, the value of the DSCP field makes it possible to identify the flow type (real time/elastic time, voice/data, etc.), but, in no case, the level of
30 criticality of the flow. Furthermore, switching policies can be applied only to all of the traffic going from one encryptor to another; there is no longer visibility concerning the subscribers or group of subscribers.

35

Figure 3 illustrates the routing of the flows in a network of the type of that of figure 2.

Each standalone system implements IGP (Interior Gateway Protocol) and EGP (Exterior Gateway Protocol) routing protocols to route the flows. One example of IGP
5 protocol is the BGP protocol (Border Gateway Protocol). One example of EGP protocol is the OSPF protocol.

The standalone systems representing the enclaves S1, S2, S3, S4 implement the OSPF protocol in a routing
10 domain which comprises the red routers R1_S1, R1_S2, R1_S3, R1_S4 but excludes the encryptors Z_S1, Z_S2, Z_S3, Z_S4. The encryptors do not implement the OSPF protocol and are not capable of establishing a routing topology from the source (themselves) to the
15 recipients. The routing of the flows in the encryptors is performed by the Security Policy (SP) and Security Association (SA) routing policy, information contained in the SPD database ("Security Policy Database").

20 The black routers R2_S1, R2_S2, R2_S3, R2_S4 implement the OSPF protocol to make it possible to take account, in the complex architectures, of an independent administrative entity of the main site, but using the resources common to the different WANs, the QoS routers
25 being managed (Administration/Supervision) by the entity of the main site. The set comprising the QoS routers of the sites of the same organizational entity form a transit federator with respect to the serving sites that they connect, and do so for a given flow
30 category (sensitive or non-sensitive).

The BGP protocol is implemented between the routers R2_S1, R2_S2, R2_S3, R2_S4 and the networks WAN_M and WAN_C. It makes it possible to communicate to the
35 different WANs the prefixes of the subnetworks present in the serving networks.

The WAN networks implement a routing protocol (OSPF for example). It handles the routing of the flows between the different interconnected serving networks. This protocol makes it possible to establish a routing topology by assigning costs to the paths taken, the choice of the route being that of least cost. The prefixes indicated in the routing tables of the routers of the WAN networks are the prefixes of the black addresses of encryptors, the addresses of the user plan being masked by the encryptors.

The OSPF protocol is a link state protocol; to operate, it requires the routers which use this protocol to be adjacent, which can be translated as meaning "be connected by a direct link"; now, the encryptors do not make it possible to have a direct link between an unprotected entity and a protected entity. To re-establish connectivity between the routers R1_S1, R1_S2, R1_S3, R1_S4 it is necessary to use GRE tunnels, then to implement the OSPF protocol on these "GRE interfaces". The GRE tunnels are implemented as an overlay on the IPsec layer (ESP protocol) and they generate an overhead of four additional bytes. Consequently, it is possible to reconstruct an OSPF routing topology between the serving networks through the GRE tunnels.

The quality of service management is implemented in the routers R2_S1, R2_S2, R2_S3, R2_S4. In each router, it has to conform to the quality of service policy with respect to the WAN networks, WAN_M and WAN_C, as well as that of the routers R1_S1, R1_S2, R1_S3, R1_S4, installed on the site for the benefit of the administrative entities. The overall consistency of the quality of service for the benefit of a collective user which has to convey the sensitive and non-sensitive flows can be achieved only through independent QoS

router configuration operations, each router having to process sensitive or non-sensitive flows.

One aim of the invention is to resolve at least one of the abovementioned problems. The proposed solution makes it possible to take the routing decisions before encrypting the information and to integrate in one and the same product all the functions necessary to the interconnection of the MAN to the WANS. The routing guidelines are established on the red side of the network and are applied on the black side.

One advantage of the proposed solution is to be able to perform the interconnection of a MAN with WANS by adding operational resilience functions. The use of the router according to the invention for managing secure data flows notably comprises the following advantages:

- enabling cooperation between the red routing plans and the setting up of the IPsec tunnels;
- allowing simultaneous use of the two WAN networks by taking account of the "instantaneous" characteristics of these WANS, resource occupancy rate, packet transit delays, jitter (QoS indicators);
- switching the flows from the serving networks according to the states of the WANS and according to the nature of these flows (priority, flow type, etc.);
- guaranteeing the routing of a certain flow category (vital flows);
- guaranteeing the quality of service from end to end, from user to user;
- offering operational resilience functions;
- ensuring routing consistency from end to end on secure VPN networks;
- optimizing the transit resources.

The subject of the invention is notably a system for

managing secure flows transmitted between a first local area network (S1) and at least one second local area network (S2) interconnected via a plurality of wide area networks WAN (WAN M, WAN C), characterized in that
5 said system comprises at least:

- o an observation module (OB) receiving the data flows transmitted from said first local area network (S1) and intended for at least one of said second local area networks (S2), said observation module (OB)
10 being suitable for associating with each packet of said flow a tattoo making it possible to identify the data flows uniquely,
- o a module (CH) for encrypting said packets tattooed by said observation module (OB), the encryption
15 operation excluding the tattooed information,
- o a module (AN) for qualitatively and quantitatively analyzing the data flows transmitted from said first local area network (S1) making it possible to rank the flows according to their degree of priority
20 and/or of security, this degree being determined at least on the basis of the source, of the destination or of the type of user of the flow,
- o an interface module (IN) performing on the one hand the setting up and the maintaining of point-to-point
25 or point-to-multipoint data links between said first local area network (S1) and at least one of said remote local area networks (S2), each data link using the transmission means provided by one or more of said wide area networks WAN and supplying
30 communication characteristics within an operating band that are predetermined, and on the other hand the switching of the secure flows over these links according to rules consistent with the tattooing operations of said observation module (OB) and
35 encryption operations of said encryption module (CH),
- o a decision module (DE) associating with each data flow, according to their degree of priority and/or of

security determined by the analysis module (AN), a predetermined data link out of the data links set up by said interface module (IN) and according to the probability of correct routing of a flow taking each
5 data link set up by said interface module (IN),
o a module (ALS) for lexically and syntactically analyzing the messages transmitted between said decision module (DE) and said interface module (IN) so as to ensure a partitioning of the exchanges
10 between said first local area network (S1) and said wide area networks (WAN).

In a variant embodiment of the invention, said observation module (OB) performs the tattooing of the
15 flows by modifying the value of the DSCP field of the IP packets contained in said flows.

In a variant embodiment of the invention, said encryption module (CH) implements the IPsec protocol in
20 tunnel mode.

In a variant embodiment of the invention, said flows are associated with a data link using a private wide area network (WAN_M) or a public wide area network
25 (WAN_M) according to the nature of their source.

In a variant embodiment of the invention, the flows for which the degree of priority is the highest are associated with the data links benefitting from the
30 highest available bit rate.

Another subject of the invention is a method for managing secure flows transmitted between a first local area network (S1) and at least one second local area
35 network (S2) interconnected via a plurality of wide area networks WAN (RW1, WAN M, WAN C), said local area networks (S1, S2) comprising at least one input/output

interface I1, said wide area networks WAN comprising at least one input/output interface I2, I3, said method being characterized in that it comprises at least the following steps for each local area network (S1, S2):

- 5 o defining a plurality of functions F1 to F9 which can be integrated on a single hardware and/or software platform connected to said interfaces I1, I2, I3 of said local and wide area networks,
- 10 o the function F1 handles the IPsec protection of the flows from the interfaces I1 and intended for the interfaces I2 and I3, the function F1 being broken down into subfunctions F1.1 to F1.n, n representing the number of wide area networks WAN,
- 15 o the function F2 handles the setting up of a plurality of point-to-point links between said hardware platforms connected to the input/output interfaces of each local area network (S1, S2),
- 20 o the function F3 handles the switching, according to their characteristics, of the flows from and intended for the interface I1 of said local area network (S1) by separating the session mode flows from the other flows,
- 25 o the function F4 handles the processing of the session mode flows,
- 30 o the function F5 handles the processing of the exchanges between the function F1 and the function F4, notably by indicating to the function F1 the starts, ends and numbers of sessions contained in said flows,
- 35 o the function F6 handles the processing of the congestions,
- o the function F7 handles the interworking with the wide area networks WAN, by recovering the traffic engineering information (TE), by summarizing said information and by communicating said information to the function F1,
- o the functions F2, F3, F4 and F5 are network functions

whose administration is handled by the function F8,
o the function F9 handles the administration of the
security functions such as the function F1.

- 5 Other features will become apparent on reading the
following detailed description given as a nonlimiting
example in light of the appended drawings which
represent:
- 10 - figure 1, an example of an architecture of a system
according to the prior art,
 - figure 2, another illustration of the exemplary
architecture of figure 1,
 - figure 3, an illustration of the routing of the data
flows in a network of the type of figures 1 or 2,
 - 15 - figure 4, a block diagram of the general architecture
of the system according to the invention in a first
embodiment,
 - figure 5, an exemplary implementation of a first
function F1 of the method according to the invention
20 in the first embodiment,
 - figure 6, an exemplary implementation of a second
function F2 of the method according to the invention
in the first embodiment,
 - figure 7, an exemplary implementation of a third
25 function F3 of the method according to the invention
in the first embodiment,
 - figure 8, an exemplary implementation of a fourth
function F4 of the method according to the invention
in the first embodiment,
 - 30 - figure 9, an exemplary implementation of a fifth
function F5 of the method according to the invention
in the first embodiment,
 - figure 10, an exemplary implementation of a sixth
function F6 of the method according to the invention
35 in the first embodiment,
 - figure 11, an exemplary implementation of a seventh
function F7 of the method according to the invention

in the first embodiment,

- figure 12, an exemplary implementation of an eighth function F8 and of a ninth function F9 of the method according to the invention in the first embodiment,
- 5 - figure 13, a block diagram of the architecture of the system according to the invention in a second embodiment.

The transfer of data by IP networks is not subject to
10 any guarantee of routing and of handover of these data to a final user; this Best Effort mode of operation is the nominal mode of operation of IP networks, apart from a few specific functionalities built on the processing of the DSCP field of the IP packet,
15 associated with management of queues allowing a priority routing of certain IP packets over others.

To guarantee the routing of the data, it is implicitly necessary, on the one hand, to establish a permanent
20 relationship between the two ends (users) for the duration of the communication. Only a connected mode of operation makes it possible to guarantee this relationship and, on the other hand, to proceed with a resource reservation on the WAN networks corresponding
25 to the needs of the communication on the path thereof, these resources being reserved in each equipment element involved in the communication.

There now follows a description, based on figures 4 to
30 12, of a first embodiment of a method and a system for managing secure flows in a network according to the invention.

Figure 4 illustrates the architecture of the system
35 according to the invention in a first embodiment.

The architecture of the system according to the

invention implements a set of functions in order to resolve the limitations of the known network architectures as illustrated in figures 1 and 2. In particular, the invention makes it possible to ensure a
5 secure interconnection between one or more local area networks LAN and one or more public or private wide area networks WAN.

The system according to the invention is interfaced, on
10 the one hand with a first local area network S1 via an interface I1 and, on the other hand with the available wide area networks WAN, via a plurality of interfaces I2, I3, In, to set up a point-to-point link between said first local area network S1 and one or more other
15 remote local area networks S2.

A function F1 handles the secure protection, for example through the IPsec protocol, of the flows from the interfaces I1 and intended for the interfaces I2
20 and I3. The function F1 is broken down into subfunctions F1.1 to F1.n, n representing the number of wide area networks WAN interfaced with the method. An interface Ix is assigned to a subfunction F1.x.

25 A function F2 handles the setting up of a plurality of point-to-point links of predetermined transfer characteristics between the system according to the invention connected to the first local area network S1 and the remote systems connected to the other local
30 area networks S2.

A function F3 handles the switching and the recognition of the flows from and intended for the interface I1. The switching of the flows separates the flows in
35 session mode from the other flows.

A function F4 handles the processing of the flows in

session mode.

5 A function F5 handles the processing of the relationships between the function F1 and the function F4. It makes it possible, notably, to indicate the function F1, the starts and ends of sessions as well as the numbers of the sessions.

10 A function F6 handles the processing of the congestion aspects and the processing of the aspects relating to the traffic engineering (TE) and controls the switching of the flows recognized by the function F3 on the links set up by the function F2 according to the congestion states that it detects.

15 A function F7 handles the interworking with the black WANs by translating the flows passing through the function F1 so as to equate the point-to-point links set up by the function F2 with paths managed by the
20 wide area networks WAN. It is also responsible for recovering the TE information from the black WANs, for summarizing said information and for communicating said information to the function F1.

25 A function F8 handles the administration of the network functions. The functions F2, F3, F4 and F5 are network functions.

30 A function F9 handles the processing of the security functions. The function F1 is a security function.

Databases are associated with these functions; they make it possible to store the information specific to the network and security functions, or information
35 common to both of these functions. These databases, called MIB ("Management Information Base") databases, are as follows:

- An MIB database BD1 which is dedicated to the operations of administering and supervising the network functions, accessible in read and write mode by the function F8.
- 5 • An MIB database BD2 which is dedicated to the operations of administering and supervising the security functions, accessible in read and write mode by the function F9.
- An MIB database BD3, common to the network and
10 security functions, accessible in read mode only.

Figure 5 shows an exemplary implementation of the first function F1 of the method according to the invention. The local area networks S1, S2 are each interconnected
15 to the wide area networks WAN_M, WAN_C via a system 501, 502 according to the invention which implements the abovementioned functions. The incoming and outgoing flows of the local area networks LAN/MAN over the interfaces I1 require protection. This protection is
20 ensured by the implementation of the function F1. The function F1 is an IPsec function in tunnel mode. It is implemented for each interface I2, I3 between the system 501, 502 according to the invention and the wide area networks. In the example of figure 5, two
25 functions F1, respectively denoted F1.1, F1.2, are implemented for each interface I2, I3. The tunnels are set up dynamically between the functions F1.1, F1.2 executed by the remote systems 501, 502. The function F1 implements a method for automatic discovery of the
30 remote methods. It handles the authentication of the remote methods, and the maintaining of the connectivity of the IPsec tunnels between the local and remote entities F1.1, F1.2.

35 Figure 6 presents an exemplary implementation of the second function F2 of the method according to the invention. The use of IPsec tunnels set up through WAN

networks entails positioning other GRE tunnels in overlay on these IPsec tunnels, this principle not being extendable to large network topologies. To overcome this defect, the proposed solution is to use
5 an "underlay" function, that is to say, to work at the level below IPsec to establish the relationships between remote entities. This function designated F2 makes it possible to set up a point-to-point link between two remote units, the MPLS ("Multi-Protocol
10 Label Switching") protocol is one of the protocols that makes it possible to satisfy this function. Other techniques such as virtual local area networks VLAN can also satisfy the function F2. The links between the functions F2 are set up on the interfaces I2 and I3.
15 The information sent or received by this function F2 takes the interfaces I2 and I3.

Figure 7 presents an exemplary implementation of the third function F3 of the method according to the
20 invention. The function F3 is in a "full duplex" relationship with the interface I1, that is to say in simultaneous bidirectional communication. The flows from the interface I1 are switched according to their characteristics to the function F4 or to the function
25 F2. The flows in session mode, such as the SIP protocol ("Session Initiation Protocol") for example, are switched to the function F4, the other flows being switched to the function F2.

30 The function F3 also makes it possible to extend to the system according to the invention the partitioning characteristics between users, such as the virtual networks VLAN ("Virtual Local Area Network") or the virtual routing tables VRF ("Virtual Routing and
35 Forwarding Table"). These characteristics can be routed by the local method to the remote methods.

Figure 8 presents an exemplary implementation of the fourth function F4 of the method according to the invention.

- 5 The function F4 receives only the flows in session mode from the function F3 (for example the SIP protocol). The function F4 interprets the "session" protocol and it identifies in the protocol the field which carries the MLPP information indicating the priority of the
10 session, this information having been forged in the field concerned (the RP field in the case of the SIP protocol) by functional entities of the local area network LAN/MAN. An RSVP ("Resource ReSerVation Protocol") or RSVP-TE ("Resource ReSerVation Protocol-
15 Traffic Extension") request dependent on the underlying wide area network WAN is generated to the function F4 of the remote method that is the recipient of the session via the function F3.
- 20 The function F4 implements an Internet routing protocol of IGP ("Interior Gateway Protocol") type having the capacity to set up a topology of links including metrics notably of bandwidth availability and occupied band. The OSPF-TE protocol is one of these protocols
25 which can be suited to this function part. Associated with this Internet routing protocol, a better path computation subfunction taking account of the metrics mentioned above makes it possible to define the best routes to reach the remote secure flow management
30 systems. The C-SPF subfunction is one of the functions that makes it possible to satisfy this computation. The information derived from C-SPF is indicated as parameters in the RSVP-TE request. The function F4 generates RSVP or RSVP-TE requests only to the WAN
35 networks which accept these requests.

Figure 9 presents an exemplary implementation of the

fifth function F5 of the method according to the invention. The function F5 enables dialog between the functions F4 and each function F1.1, F1.2. This function is a control function which sends and/or
5 receives messages from or intended for the functions F4 and F1. The messages are conveyed by the UDP protocol ("User Datagram Protocol"). The main messages make it possible to send and receive information on the communication sessions to be opened, to be closed, or
10 on the behavior required with regard to the communications on the basis of parameters obtained from the function F1 and notably from its "black interface" part. The function F5 makes it possible to make the link between the session number (for example, an LSP
15 number) and an IPsec context (for example, an SPI, "Security Parameter Index", number), information that is contained in the SDP.

Figure 10 presents an exemplary implementation of the
20 sixth function F6 of the method according to the invention. The function F6 is related to the functions F3, F4. It implements a number of means and mechanisms for managing the congestions or influencing the processing of the flows, the operations implemented by
25 the functions F4 and F6 being called "flow processing policy".

The function F4 has all the contexts of the sessions that are established or being established, as well as
30 the priority levels of these sessions. In nominal operation, the flows are routed to the WAN networks that are present in "active - active" mode, that is to say that the routing chooses one of the WAN networks depending on the types of flow to be routed and the
35 constraints associated with these flows. This principle makes it possible to use all the capacities of the WAN networks at the same time without operation of the

"active - backup" type. In case of congestion signaled to the function F6, the main methods used to influence the processing of the flows are as follows, this list not being exhaustive:

- 5 • DiffServ mode: the routing of the flows is performed according to the DSCP field and according to a number of classes of service;
- ECN Bit mode: a congestion signaled on the positioning of the ECN bit on a session or a class of
10 service of the "data" type provokes a change of the routing path for the flows affected by this congestion;
- SAA mode: the function implements tools that make it possible to measure certain characteristics of the
15 flows through the WAN networks. These tools make it possible to measure the jitter, the transit delay, the latency, and do so on each of the WAN networks. The analysis of the results may provoke a change of the routing path for the flows affected by the
20 analysis of the metrics, if the latter have values outside the limits prescribed in the service level agreement "SLA";
- "Denial of service" mode. A denial of service attack is detected by the function F1 and signaled to the
25 function F4 through the function F5 is retransmitted to the function F6 which provokes a change of the routing path for the flows affected by this attack.

Figure 11 presents an exemplary implementation of the
30 seventh function F7 of the method according to the invention. The flows incoming and outgoing from and to the WAN networks over the interfaces I2, I3 are conveyed to these interfaces by the function F7. The function F7 is duplicated in as many functions (F7.1 to
35 F7.n) as there are WAN networks, this duplication making it possible to make the actions and processing operations independent on the WAN networks.

The function F7 handles a number of subfunctions, and notably:

- An Isec overhead management subfunction. The
5 function F7 takes account of the overhead imposed by
the IPsec encryption implicitly through a management
command communicated by the function F6. The overhead
is expressed as a number of additional bytes to be
10 taken into account in the computation of the quality
of service. The function F7 expresses a user need in
terms of bandwidth corresponding to the SLA ("Service
Level Agreement") requested by the user, and this
expression of need is made according to the classes
of services. A computation is performed by the
15 function F7 to check the consistency between the
physical bit rates of the interfaces of the local
area networks LAN/MAN and those of the wide area
networks WAN, and the requests expressed by the user
in the expressed classes of services.
- A subfunction for computing the best paths to be used
20 on the WAN network from the function F7.1, F7.2
concerned and by taking into account the metrics of
TE type (OSPF-TE and MPLS-TE).
- A subfunction related to the ECN ("Explicit
25 Congestion Notification") extension of the Internet
protocol, for the computation of the congestion,
number of packets congested, session number affected,
etc.

30 The information obtained is specified in a message
intended for the function F5. The function F1
retranscribes this information to the function F5. The
messages are of the TLV ("Type Length Value") type, the
function being represented by the "T" (Type) field.

35

Figure 12 presents an exemplary implementation of the
eighth function F8 and of the ninth function F9 of the

method according to the invention.

All the functions F1, F2, F3, F4, F5, F6 and F7 are implemented on a common hardware and software base. The
5 NOC and SOC administration functions can coexist more easily, which makes it possible to have MIB databases dedicated to an operating domain, a network MIB base and a security MIB base as well as a common MIB base containing the "network" information and the "non-
10 sensitive security" information. The sensitive information such as the cryptology elements (keys) are contained in the MIB base dedicated to security. Because of this, the security information is always accessible and it requires no additional equipment for
15 its accessibility.

The system according to the invention combines all the functions. It constitutes a single and unique standalone system (SA). Its administration is handled
20 by a WAN standalone system or by a MAN standalone system. To facilitate the follow-up of the service level agreements SLA, information from the network and security administration MIB base (common MIB base) can be accessed in read mode only by the standalone system
25 which is not responsible for the administration of the method, in order to provide a view of the quality of service to the standalone system which does not handle this administration.

30 The function F8 is related to the functions F2, F3, F4, F5 and F6 to perform the operations of administration (configuration) and supervision of these functions. The function F9 is related to the function F1 and F7 to perform the functions of administration (configuration)
35 and of supervision of this function. The function F8 is related to the database BD1. The database BD1 is in read and write mode. The function F9 is related to the

database BD2 and the database BD2 is in read and write mode. Finally, the database BD3 receives information from the database BD1 and BD2, the database BD3 being in read mode only.

5

To sum up, according to one implementation, in a first embodiment of the method for managing secure flows according to the invention, the following steps are executed:

- 10 • using the IPsec protocol in tunnel mode to implement the function F1 and the subfunctions F1.x;
- using a point-to-point level 2 protocol between the function F2 of the local method and the remote methods. The MPLS protocol is a protocol that is a
15 candidate for this function;
- using a level 2 protocol between the function F2 and the function F1. The 802.1Q (VLAN) protocol is this protocol. The VLAN number makes it possible to establish a correlation with the SPI number, the
20 identifier of the session encryption context;
- switching the flows from the local area networks LAN/MAN to the function F4 and/or to the function F2. The switching to the function F4 relates to the flows in session mode;
- 25 • generating, via the function F4, RSVP requests to the function F1. The function F1 interprets this request, directs it to the remote end through the IPsec tunnel considered and the function F1 generates, to the black wide area network WAN, the RSVP request which
30 bears the attributes of the context of the session;
- using a communication protocol between the functions F1 and the function F5 to allow the exchange of signaling messages between these functions and notably the information relating to the numbers of
35 the sessions between the local and remote methods;
- communicating to the function F4 and F6, via the function F5, the information from the function F1;

- using, by the function F6, the information obtained from the function F7 and from the subfunctions F7.x retransmitted via the function F1. This information is conveyed in the form of messages and contains the
5 Quality of Service information derived from the black wide area networks WAN;
- proceeding with the analysis of the information from the black wide area networks WAN via the function F7 and the subfunctions F7.x. Communicating this
10 information to the function F1;
- switching the flows to the functions F1.x according to the analysis of the information received or proceeding with the pre-emption of the current sessions in order to release resources;
- 15 • filtering the information from the function F7 by the function F1 and communicating this information to the function F5;
- administering the network information from the functions F2, F3, F4, F5 and F6 via the function F8
20 and storing this information in a database (BD1). Making this information accessible in read and write mode by the designated functions;
- administering the security information from the functions F1, F7 via the function F9 and storing this
25 information in a database (BD2). Making this information accessible in read and write mode by the designated functions;
- having the network (BD1) and security (BD2) databases communicate to extract the common information and
30 store it in a database (BD3). Making this information accessible in read mode only by the designated functions;

the functions F1 to F9 being integrated on a single hardware and software platform.

35

The distribution of the functions F1 to F9 can also be produced with different hardware and software

platforms. The communication protocol between these platforms is a level 2 protocol.

5 According to an implementation of the method according to the invention, the switching of the flows to the function F4 relates to all the flows in session mode and all the flows in non-session mode.

10 According to an implementation of the method according to the invention, the information obtained from the function F7 concerning traffic engineering (TE) information is transmitted to the function F6 via the function F1.

15 According to one implementation of the method according to the invention, the administration of the network and security information is consolidated in a single database.

20 The method according to the invention comprises multiple advantages:

- an improvement in the resilience of the communications and services;
- an optimization of the leased transmission resources
- 25 (operator VPNS);
- the possibility of implementing mechanisms for the pre-emption of the vital flows and therefore ensuring the guarantee of routing of the vital flows;
- an improvement in the quality of service to all the
- 30 flows by discriminating the flow types according to the uses.

It carries out the routing operations and notably the choice of the route to reach the target before carrying

35 out the encryption operations by taking account of qualitative criteria concerning the state of the paths taken (quality of service, transit delays, rate of

occupancy of the resources, packet loss, for example). It requires a close collaboration between the encryption entities and the routing entity.

- 5 The invention is now described in a second embodiment illustrated by the block diagram of figure 13.

The system 100 according to the invention implements the method for managing secure flows described above.
10 The system 100 enables, notably, a secure interconnection of a first local area network S1 with a plurality of other remote local area networks through public or private wide area networks WANs.

- 15 The system 100 comprises an observation module OB which receives the flows from the local area network S1 and transmits them to an encryption device CH which handles the function of securing said flows, for example using the IPsec protocol. The encrypted flows are then
20 transmitted to an interface module IN which switches the flows to one or more wide area networks WAN on the basis of predetermined criteria.

The system 100 also comprises an analysis module AN
25 which receives a copy of each packet received by the observation module OB and which identifies flows and associates a degree of priority and/or of security as well as requirements in terms of quality of service with them, and a decision module DE which receives
30 information from the analysis module AN concerning each of the identified flows and information on the availability of point-to-point or point-to-multipoint links between interface modules IN and of predetermined characteristics via a lexical and syntactic analysis
35 module ALS.

One of the aims of the system 100 according to the

invention is to ensure a switching of the flows transmitted from the local area network S1 to one or more wide area networks WANS by ensuring a differentiation of the services and a transmission of
5 each flow to the wide area network WAN that is best suited on the basis of predetermined constraints and the state of these wide area networks. The difficulty with such an adaptation lies in the presence of the encryption device CH which imposes a partitioning
10 between the flows on the red side (local area network) and on the black side (wide area network) and therefore a prevention of exchange of information between the red routers R1_S1 and the black routers R2_S1.

15 Each module of the system 100 according to the invention is now described in more detail.

The observation module OB performs two functions. The first function consists in duplicating each packet
20 received from the local area network S1 and in transmitting a copy of each packet to the analysis module AN. The second function consists in associating with each packet, a specific tattoo in the form of a field of the header of the packet or of the frame which
25 transports this packet during the exchanges between modules so as to identify the flows uniquely in the rest of the processing operations performed by the different modules. The identification of the flows makes it possible to take into account the transmission
30 constraints specific to each flow. The expression "transmission constraint" should be understood notably to mean the bit rate required for the routing of the flow to its destination or the constraints in terms of delay, jitter or packet loss rate that a flow can
35 support while guaranteeing its routing or else the degree of security which has to be taken. Based on these transmission constraints, the transmission medium

is chosen, in this case one of the links from module IN to module IN through the available wide area networks WANS that is best suited to each flow so as to guarantee its routing to its destination. The tattooing
5 of each packet is done, for example, by modifying the value of the DSCP (Differentiated Services Code Point) field of an IP packet or by fixing MAC addresses of the frame transporting the packet.

10 The observation module OB also executes the function F3 described previously for the first embodiment of the invention.

The encryption module CH ensures the security of the
15 data flows by an encryption in tunnel mode. The tunnels are set up dynamically between each encryption module of each system connected to a source or destination local area network. The packets transmitted by the observation module OB are fully encrypted and
20 encapsulated in a packet or a frame where the identification of the flow will be at least locally legible, for example through the DSCP field of the encapsulating packet.

25 The encryption module CH also executes the function F1 described previously for the first embodiment of the invention.

The analysis module AN performs a qualitative and
30 quantitative analysis of the flows circulating between the local area network S1 and the remote LAN networks. This analysis makes it possible to anticipate the needs and to judge the good fit between needs and interconnection means in place. Each identified flow
35 has flow constraints to be observed associated with it. Based on predefined categories, the analysis module AN associates the degree of priority of the flow with a

minimum bandwidth need. The analysis of the degree of priority of a flow is performed, for example, by an interpretation of the "session" protocol by identifying the field which bears the information indicating the
5 priority of the session which is determined by functional entities of the MAN network.

The analysis module AN also executes the function F4 described previously for the first embodiment of the
10 invention.

The decision module DE establishes the policy for switching the flows to the wide area network WAN that is best suited on the basis, on the one hand, of the
15 flow constraints to be observed for each of the flows and of the number of flows to be served determined by the analysis module AN, and on the other hand of the observed availabilities of the wide area networks WAN. The decision module DE thus determines the transport
20 services which have to be initiated, modified or cancelled in accordance with the established switching rules. To this end, it generates suitable messages allowing a secure communication of the switching choice to the interface module IN. The messages generated by
25 the decision module DE must guarantee the partitioning of the data flows between the black part and the red part of the network. In particular, the messages transmitted between the decision module DE and the interface module IN must not be correlated with the
30 data flows which transit between the local area network S1 and the wide area networks WAN. To guarantee the partitioning between red and black parts of the network, the decision module DE implements a set of checks, of state machine type. The decision module DE
35 also takes into account, in the assignment of the flows to a WAN network, the overhead added by the encryption module CH. This overhead is notably taken into account

for the computation of the transmission bit rate required for the routing of a flow according to its degree of priority.

- 5 The decision module DE also executes the functions F6 and F7 described previously for the first embodiment of the invention.

10 The lexical and syntactic analysis module ALS analyzing the messages exchanged between the decision module DE and the interface module IN makes it possible to produce a partitioning between the red and black parts of the network. The messages from the interface module IN are accepted by the module ALS only if they
15 intervene in response to an explicit request formulated by the decision module DE. These messages notably contain the encrypted packet header attributes which make it possible to identify the link used out of the available WAN networks and the characteristics of this
20 link. The lexical and syntactic analysis module ALS constitutes a secure gateway that makes it possible, on the one hand, to inform the interface module IN of the switching decisions taken by the decision module DE and, on the other hand, to indicate to the decision
25 module DE the state of the links set up by the wide area networks WANS.

The security established by the module ALS makes it possible to withstand the denial of service attacks
30 potentially originating from the wide area networks WANS. It also guarantees the absence of information leaks.

The lexical and syntactic analysis module ALS also
35 executes the function F5 described previously for the first embodiment of the invention.

The interface module IN sets up point-to-point or point-to-multipoint links between the local area network S1 and at least one other remote network S2 through one or more wide area networks WAN. It ensures
5 that each link is operating within the predetermined operating band and on which the decision module DE has established its switching policy. It supplies the availability state of the established links to the decision module DE, via the module ALS. The setting up
10 of point-to-point or point-to-multipoint links is done, for example, using the MPLS (Multiprotocol Label Switching) data transport mechanism or by the introduction of virtual networks VLAN. Based on the messages transmitted by the decision module DE, the
15 interface module IN can apply the established switching policy, for each encrypted flow, according to its identification. A link is characterized on the one hand by the identifiers of the local area networks S1, S2 that it connects and on the other hand by the data
20 transfer parameters on this link. These parameters are notably the transfer delay, the average packet loss rate, the security level, the criticality level, the maximum continuous bit rate, and the maximum service interruption time. A link is identified by a
25 combination of encrypted packet header attributes, notably including the DSCP field and the source and destination addresses of the flow. A link is maintained in accordance with its predetermined characteristics. For example, in the case of malfunction of a WAN
30 network, the link can be maintained by using other transmission means, for example satellite transmission means.

The interface module IN also implements an IGP link
35 state routing protocol that has the capacity to set up a link topology including metrics of bandwidth availability and occupied band. For example, a routing

protocol suited to this purpose is the OSPF-TE
protocol. In association with this protocol, a shortest
path computation function is executed. It takes account
of said metrics in order to define the best routes to
5 reach the destination network.

The interface module IN also executes the functions F2,
F4 and F7 described previously for the first embodiment
of the invention.

10

The system 100 according to the invention and the
modules of which it is made up are implemented on a
common hardware and/or software base.

CLAIMS

1. A system (100) for managing secure flows transmitted between a first local area network (S1) and at least one second local area network (S2) interconnected via a plurality of wide area networks WAN (WAN M, WAN C), characterized in that said system (100) comprises at least:
- o an observation module (OB) receiving the data flows transmitted from said first local area network (S1) and intended for at least one of said second local area networks (S2), said observation module (OB) being suitable for associating with each packet of said flow a tattoo making it possible to identify the data flows uniquely,
 - o a module (CH) for encrypting said packets tattooed by said observation module (OB), the encryption operation excluding the tattooed information,
 - o a module (AN) for qualitatively and quantitatively analyzing the data flows transmitted from said first local area network (S1) making it possible to rank the flows according to their degree of priority and/or of security, this degree being determined at least on the basis of the source, of the destination or of the type of user of the flow,
 - o an interface module (IN) performing on the one hand the setting up and the maintaining of point-to-point or point-to-multipoint data links between said first local area network (S1) and at least one of said remote local area networks (S2), each data link using the transmission means provided by one or more of said wide area networks WAN and supplying communication characteristics within an operating band that

- 40 -

- are predetermined, and on the other hand the switching of the secure flows over these links according to rules consistent with the tattooing operations of said observation module (OB) and encryption operations of said encryption module (CH),
- 5 o a decision module (DE) associating with each data flow, according to their degree of priority and/or of security determined by the analysis module (AN), a predetermined data link out of the data links set up by said interface module (IN) and according to the probability of correct routing of a flow taking each data link set up by said interface module (IN),
- 10 o a module (ALS) for lexically and syntactically analyzing the messages transmitted between said decision module (DE) and said interface module (IN) so as to ensure a partitioning of the exchanges between said first local area network (S1) and said wide area networks (WAN).
- 15 2. The system (100) for managing secure flows as claimed in claim 1, characterized in that said observation module (OB) performs the tattooing of the flows by modifying the value of the DSCP field of the IP packets contained in said flows.
- 20 3. The system (100) for managing secure flows as claimed in one of the preceding claims, characterized in that said encryption module (CH) implements the IPSec protocol in tunnel mode.
- 25 4. The system (100) for managing secure flows as claimed in one of the preceding claims, characterized in that said flows are associated with a data link using a private wide area network (WAN_M) or a public wide area network (WAN_M)
- 30
- 35

- 41 -

according to the nature of their source.

5. The system (100) for managing secure flows as
claimed in one of the preceding claims,
5 characterized in that the flows for which the
degree of priority is the highest are associated
with the data links benefitting from the highest
available bit rate.