Selecting an ATM or IP Security Solution to Secure an IP over ATM Virtual Private Network

Maryline Laurent-Maknavicius

INT, Institut national des télécommunications
9, rue Charles Fourier - 91 011 Evry Cedex – France
Maryline.Maknavicius@int-evry.fr

ABSTRACT

In 1999, the ATM Forum international consortium approved the first version of its ATM security specifications, whereas the Internet Engineering Task Force (IETF) published a series of IP security RFC. The aim of those documents is to protect communications over Asynchronous Transfer Mode (ATM) network, respectively the Internet Protocol (IP) network by offering data confidentiality, partners authentication, etc. This paper considers an IP/ATM VPN environment and addresses the best security services placement either in the IP or ATM protocol and the positioning of those security solutions in the architecture. Traffic filtering aspects are also considered.

I. INTRODUCTION

In an environment of IP over ATM Virtual Private Network (VPN), introducing security services raises the problem of their placement. Two security protocols are available, one defined by the ATM Forum through specification versions 1.0 [1] and 1.1 [2], and another known as IPsec (for IP security) defined by the IETF in RFC [3], [4], [5], [6], and [7]. For simplification purpose, the ATM security solution is referred to as AFSEC in the remainder of the paper.

A typical such architecture is presented in figure 1 and used as a basis for the present study. Equipments of site A are numbered from (a) to (e) with equipment (c) supporting an ATM videoconferencing application and other IP applications. In site A, as depicted in table 1, three security policies are possible numbered from (1) to (3) with various security perimeters. The security solution consists in positioning an AFSEC unit at the border of the site in (a), an IPsec unit in (e) and AFSEC and/or IPsec units in (b), (c), (d).

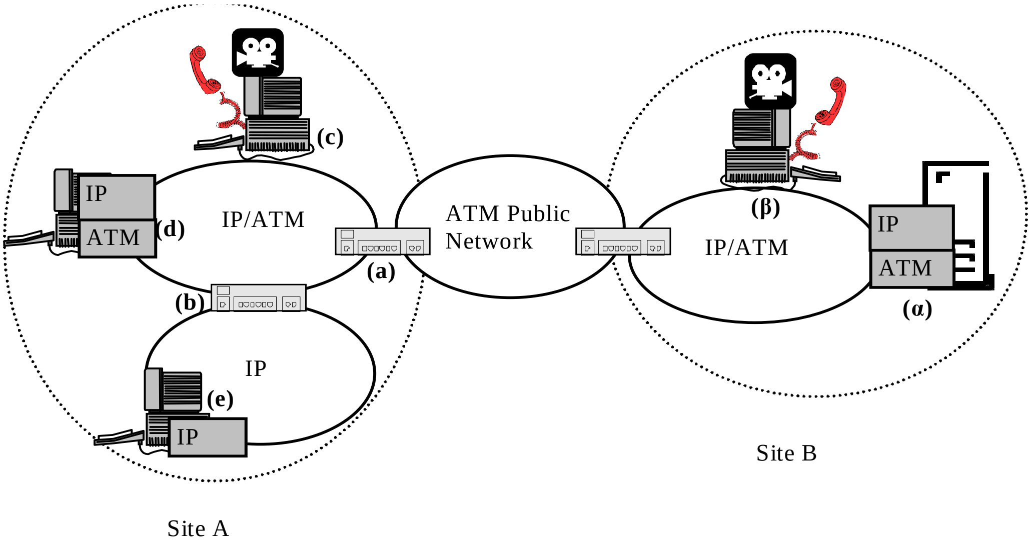

Figure 1: *An ATM-based VPN architecture example*

Security policy	Site interconnection protection **(1)**	Protection over the IP/ATM networks **(2)**	Protection over the IP and IP/ATM networks **(3)**
Positioning in the architecture of figure 1	**Security gateway in (a)**	**Security gateway in (b)** **Security unit within equipments (c) and (d)**	**Security unit within equipments (e), (c) and (d)**
Security solution	**AFSEC**	**IPsec or AFSEC**	**IPsec or AFSEC**

Table 1: *Security solution positioning and type depending on the security policy applied in site A*

If the security policy (1) aims to ensure site interconnection protection, that means that the traffic exchanged between sites should be protected over the ATM public network but not necessarily over the local networks (IP/ATM and IP). The best solution is to introduce two AFSEC security gateways, one at position (a) and another one at the border of site B. As such, the traffic between sites A and B will be protected by those security equipments. One positive point of this approach is the centralized security management offered and as such the ease of management.

With more than 70% of the overall attacks realized within a site by the employees themselves, it may be useful to protect communications within the site as proposed by security policies (2) and (3). The solution for (2) is to introduce either AFSEC or IPsec in equipments (b), (c), and (d), and additionally for (3), IPsec is required in (e). Security policies (2) and (3) allow communications internal to site A to be secured, as well as communications between one end equipment of site A and one end equipment of site B.

The next two sections give general aspects of comparison between IPsec and AFSEC. Sections 4, 5, and 6 study the best solution and positioning within the architecture for the confidentiality service, the data integrity/authentication services, and the data replay detection. Section 7 studies another security key aspect which is access control, and analyzes the best position for filtering IP and ATM traffic through a firewall. Finally section 8 gives some conclusions.

II. ADVANTAGES OF PLACING SECURITY WITHIN ATM

One of the AFSEC advantages is that it offers protection to any applications. Most of existing applications may benefit from the security defined in IPsec since based on the IP protocol. However, there are ATM native applications – like videoconferencing – known as "ATM native" since directly connected on top of the ATM stack as illustrated in figure 2. If the videoconferencing device is provided with the videoconferencing application and some IP-based applications, it appears that the only one common protection means for all the applications is AFSEC. Another solution would have been to consider IPsec for IP-based applications and to develop specific software for securing the ATM native application exchanges. Note that this latter solution requires modifying all the ATM native applications, and it is not as reliable as AFSEC since the resulted security solution is not standardized and as such may include security holes.

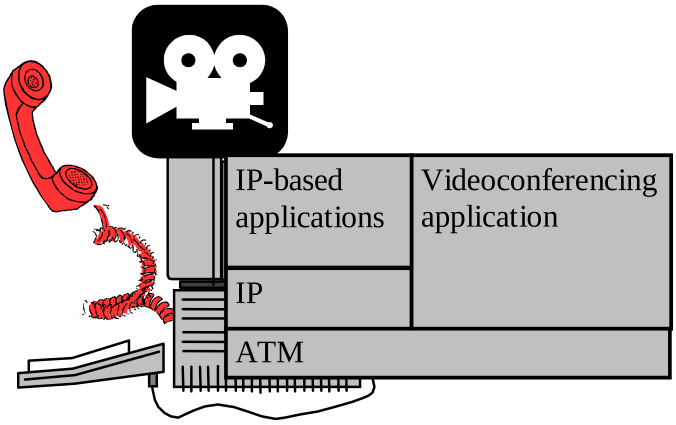

Figure 2: *The videoconferencing device*

The AFSEC processing is simpler than IPsec for security association negotiation and keying material exchange. Those two operations are done as part of the ATM protocol whereas for IPsec they operate at the application layer using protocol IKE. Actually, IKE (Internet Key Exchange), and in particular, one of its component ISAKMP (Internet Security Association and Key Management Protocol) [6] was designed to negotiate security parameters for any security protocols like IPsec, SSL (Secure Socket Layer), SHTTP (Secure HTTP), etc. Moreover, it is designed with many options and functions. As such, it appears as much more complex than AFSEC for which only two default protocols (standards ISO/IEC 9594-8 and ISO/IEC 11770-2) are available. However, its placement in the user space provides it with flexibility and ease of updates.

The session key update is simpler in AFSEC, but less secure than IPsec's. In AFSEC, the session key update is done as part of the ATM protocol using some specific management ATM cells. In IPsec, updating a session key implies that a new security association is negotiated and that the application layer and the IKE protocol are solicited. However, whereas protection in AFSEC is limited to encrypting the session keys into management cells, the IKE key update is provided with a mode known as "Perfect Forward Secrecy" ensuring that compromise of the key used to encrypt session keys does not result in all the session key compromising.

The AFSEC protocol is more efficient than the IPsec one. Since IPsec operates in a connectionless mode, each IP packet should include the 4-octet security association identifier (SPI or Security Parameters Index) so that the receiving security equipment applies the appropriate security association.

Introducing a NAT (Network Address Translation) function within a network may be disrupting in IPsec but not in ATM. Problems raise when data are protected with a digital signature calculated over one private address and when one NAT function modifies this address into one public address. The digital signature considered as invalid at the receiving side results in the data rejection. For IPsec, this problem occurs with the Authentication Header whereas AFSEC is compatible with NAT since the digital signature generation is not done over ATM addresses.

III. ADVANTAGES OF PLACING SECURITY WITHIN IP

The advantages of IPsec are mainly relative to the authentication aspects. One possibility for AFSEC authentication uses only two exchanges, meaning that the authentication is timestamp-based and as such is sensitive to the clock synchronization problem. Another possibility involves three exchanges allowing the authentication service to be based on nonces. In IPsec, up to six exchanges are possible in IKE thus supporting the nonce-based authentication, and in the main mode, one property referred to as "identity protection" is offered to protect the partners identity in confidentiality.

Another advantage is that IPsec benefits from the work done by the IETF in the public key infrastructures (PKI), and gives the possibility for partners to communicate public keys thanks to some certificates. The ATM Forum documents [1] and [2] mention a certificate infrastructure but no AFSEC solution as advanced as the IETF PKI is proposed and no references to IETF works are done.

IPsec is more efficient than AFSEC and offers many more possibilities to select a security association than AFSEC. Instead of requiring one security parameter negotiation for each new ATM connection setup, in IPsec the same security association can be used to protect several TCP connections between two peers. The selection of one security association over an IP communication may depend on the following parameters: the source/destination IP addresses, the source/destination port numbers, and the transport protocol type. In AFSEC, the selection is usually limited to the source/destination ATM addresses, however theoretically the use of some quality of service parameters is possible but requires a complex management.

IV. DATA CONFIDENTIALITY

Data confidentiality is offered by encrypting data with an encryption algorithm and a secret cryptographic key so that data remain understandable by the legitimate destination only. The advantage of AFSEC is that encryption always operates in the hardware at the ATM cell level over fixed size blocks. In IPsec, the classical solution is to consider some encryption software. However, to reach better encryption rates, another solution is to use a specific encryption hardware realizing IP packet encryption. As far as I know, encrypting fixed size blocks will always be faster than encrypting variable size packets, and as such the AFSEC encryption rate will always be higher than that obtained by any IPsec encryption unit, even if some IPsec encryption hardware is employed.

Moreover, like IPsec, AFSEC offers confidentiality for TCP/UDP level information such as the TCP port number, and the protocol type (TCP/UDP), but additionally it enables IP addresses and some ATM level information to be protected.

Referring to table 1, security policy (1) implies using an AFSEC device in (a) to encrypt all the traffic exchanged between sites. The interest is that beyond ease of centralized security management, it makes it more difficult for intruders to make intrusions from the public network. Intrusions require injecting traffic encrypted with the appropriate key, otherwise the traffic is decrypted by the encryption device (a), and rejected at the ATM equipment destination since considered as invalid after a CRC checking. Another solution would be to subvert the encryption device (a), but this seems really difficult to realize since the ATM encryption devices are specific hardware. The site A's protection can be ensured by distributing the site security within each internal equipment (c), (d) and (b) using IPsec or AFSEC. The latter solution is generally not suitable since this would require perfectly managed internal equipments with updated patches and an appropriate security policy configuration. Those aims are as much difficult to reach that the number of internal equipments increases.

Additionally to inter site protection, protection in confidentiality may be required within the IP/ATM and IP networks (security policies (2) and (3)) for instance to avoid malicious employees eavesdropping the passwords of their colleagues. One protection solution is to integrate IPsec or AFSEC encryption into equipments (b), (c), (d) and (e). Actually for (d) and (b), even for (c), IPsec seems more suitable since cheaper than the AFSEC solution and since capable of supporting required bit rates. For (c) and (b), depending on the videoconferencing application needs and traffic capacity of the IP network, it may be necessary to employ an IPsec encryption hardware.

V. DATA AUTHENTICATION/INTEGRITY

To provide data with those services, a MAC (Message Authentication Code, e.g. digital signature) calculated other these data should be appended to the emitted data. The MAC allows the destination equipment to be sure of the originator's identity and that data have not been modified during transfer.

One of the AFSEC drawback is that data authentication/integrity services can only be supported by ATM end equipments whereas possibility is given to intermediary IPsec equipments to participate in IPsec data protection.

As such, protection of the site against the data tampering and spoofing realized from the ATM public network can not be supported by an AFSEC device in (a). However, as explained in section 4, the solution is to introduce an encryption device in (a) offering the confidentiality service, and to detect data tampering and spoofing at the ATM end equipments thanks to a simple CRC. Note that another solution would be to introduce AFSEC authentication and integrity processing in end ATM devices (b), (c) and (d). However, since the authentication/integrity services are usually not supported in today's commercial AFSEC devices, and for cost reasons, it is better to introduce an IPsec protection in devices (c), (d), and (b).

If security policies (2) and (3) apply, for cost reasons and commercial reasons, the best solution is introducing IPsec in devices (b), (c), (d) and (e).

VI. DATA REPLAY DETECTION

Data replay detection enables the destination ATM security devices to detect that the same data were received several times. This service is based on sequence numbers in AFSEC and IPsec and requires the provision of the authentication/integrity services to protect the sequence number fields.

One AFSEC drawback is that like the authentication/integrity services, the replay detection can only be supported at the ATM end equipments and not in intermediary equipments.

The sequence number is 6-octet long in ATM Adaptation Layer frames, and 4-octet in IP packets and should never be used twice. For AFSEC, a new integrity key is negotiated automatically as soon as all sequence number combinations are used. For IPsec, the Security Association (SA) is updated when its lifetime expired. As such, if the SA is not updated frequently enough, the same sequence number can be used several times. For instance, assume that a security IPsec equipment protects the traffic at 2 Mbps with the same SA, and IP packets are 1500 octet length. The same sequence number will be reused after 2^32/(2*10^6/(8*1500)) seconds $\simeq$ 298 days.

Since the replay detection is closely linked to the data authentication/integrity services, nearly the same security choices apply. That is, for security policy (1), an AFSEC encryption device should be positioned in (a). However this does not preclude any intruders to capture some ATM traffic and to transmit it again towards the same destination. To detect such replay, instead of introducing the AFSEC authentication/integrity services and replay detection in ATM end equipments, for the reasons given in section 5, the best solution is to introduce IPsec in equipments (b), (c) and (d). Moreover, if replay detection is required over IP/ATM and IP networks (security policies (2) and (3)), one has only to provide equipment (e) with IPsec.

VII. ACCESS CONTROL

Access control enables a site to control the traffic exchanged between networks in order to protect resources against unauthorized use. Thanks to the security policy enforced within the site, the access control device usually called a firewall is able to identify authorized traffic from unauthorized traffic and to block the unauthorized traffic so that for instance intrusions into the site are limited, if not vanished. Traditionally, the decision whether to authorize a traffic is done based on the IP, TCP and UDP level information. However, there are commercial and academic devices [8] (referred to as ATM firewalls) that realize filtering on IP, TCP and UDP level information as well as ATM parameters such as source and destination ATM addresses, connection identifiers (Virtual Channel and Virtual Path identifiers), and service descriptors. As such, access control can be done in the IP/ATM network and/or the IP network.

To protect the whole site A from intrusions, one commercial solution is to position an ATM firewall at the border of site A. Note that if encryption is done by equipment (a), the ATM firewall should be placed behind equipment (a) in order for the firewall to filter on the unencrypted ATM traffic. At the moment, those two security functions - ATM cell encryption and ATM cell filtering – are realized by two specific equipments. The difficulty for that solution is to find an ATM firewall that considers enough ATM/IP/TCP/UDP information for filtering and that filters at high rates so that the quality of service of ATM connections is not altered too much.

Another possibility [9] to protect site A is to distribute the access control within each ATM equipment of the IP/ATM network. This solution is academic and raises the problem of modifying each ATM equipment to introduce the appropriate filtering and the problem of collecting access control information from each ATM equipment.

Additionally, the security policy of site A may require filtering the traffic exchanged between the IP/ATM network and the IP network. For a basic filtering which does not involve any proxies, no additional equipements are required. Equipment (b) which is typically a router is able to filter the traffic on IP/TCP/UDP level information.

Criterion	**AFSEC solution**	**IPsec solution**
Applications able to be protected	IP and ATM-based applications	IP-based applications
SA negotiation and keys exchange	Simple since embedded in the ATM protocol	Flexible and easy to update since realized by an application level IKE program
Session key update	Simple since embedded in the ATM protocol	Secure since soliciting the application level IKE protocol
Compatibility with NAT	NAT compatible	May be NAT incompatible
Authentication protocol	Up to three exchanges	Up to six exchanges Possibility to keep the identity secret (identity protection)
PKI	No references to any PKI given	Based on the PKI defined by the IETF
Choice for selecting one SA	Theoretically source and/or destination ATM addresse, Usually limited to the destination ATM address	Theoretically source/destination IP addresses, source/destination port numbers, transport protocol type, Usually limited to the destination IP address
Data confidentiality	Encryption bit rates greater than those offered by IPsec Confidentiality of ATM/IP/TCP/UDP level information	Confidentiality of TCP/UDP level information
Data authentication/integrity	Can only be provided in ATM end equipments	Provided within any IPsec devices
Data replay detection	Can only be provided in ATM end equipments Based on a 6-octet sequence number Replay detection maintained by negotiating new security parameters when the sequence number cycled	Provided within any IPsec devices Based on a 4-octet sequence number Replay detection not maintained when the sequence number cycled
Access control	Filtering on ATM/IP/TCP/UDP information	Filtering on IP/TCP/UDP information

Table 2: Comparison of AFSEC and IPsec solutions

VIII. CONCLUSIONS

This paper studies the best solution to offer the confidentiality, authentication, integrity and access control services and the replay detection in an IP/ATM VPN architecture. After a general comparison regarding the IPsec and the ATM security solutions, each security service is studied independently and, depending on the security policy perimeter, the selection between IPsec and the ATM security solution is argued, along with the positioning of those security functions within the architecture.

As a conclusion, it appears that the best solution to protect traffic exchanges over an ATM VPN is placing an ATM encryption device at the border of the VPN to realize data confidentiality at the ATM level. Behind this encryption device, an ATM firewall can be placed to filter incoming/outcoming traffic and to protect site A against possible intrusions. The other security services, if any, should be realized in other internal equipments introducing IPsec.

Other local network exchange protection should be ensured through IPsec, and IP traffic filters may be introduced between sub networks.

REFERENCES

[1] ATM Forum, “ATM Security Specification Version 1.0 “, af-sec-0100.001, February 1999.

[2] ATM Forum, “ATM Security Specification Version 1.1“, fb-sec-0100.002, Final Ballot, September 2000.

[3] RFC 2401, S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol “, November 1998.

[4] RFC 2402, S. Kent, R. Atkinson, “IP Authentication Header“, November 1998.

[5] RFC 2406, S. Kent, R. Atkinson, “IP Encapsulating Security Payload (ESP)“, November 1998.

[6] RFC 2408, D. Maughan, M. Schertler, J. Turner, “Internet Security Association and Key Management Protocol (ISAKMP)“, November 1998.

[7] RFC 2409, D. Harkins, D. Carrel, “The Internet Key Exchange (IKE) “, November 1998.

[8] Olivier Paul, Maryline Laurent, Sylvain Gombault, "A Full Bandwidth ATM Firewall", 6th European Symposium on Research in Computer Security ESORICS'2000, Toulouse, France, October 2000.

[9] Olivier Paul, Maryline Laurent, "An Alternative Access Control Architecture for IP over ATM Networks", 4th IFIP Conference on Communications and Multimedia Security CMS'99, Leuven, Belgium, September 1999.