Issues and Solutions When Deploying VPNs over Satellite Links

Dirk Gómez and Eriza Fazli

TriaGnoSys GmbH
Argelsrieder Feld 22, 82234 Wessling, Germany
{dirk.gomez,eriza.fazli}@triagnosys.com

Abstract. This paper summarises the issues created when deploying a virtual private network in broadband satellite systems. These issues are related to protocol enhancing, overhead, fragmentation, mobility, quality of service and network address translation. Solutions for these issues are proposed from the point of view of the satellite operator, since most depend on what degree of control it has over the network. More specifically, this paper explains which solutions can be applied when the satellite links an airplane with the ground.

Keywords: Security, VPN, IPsec, TLS, Satellite, Link, PEP, Fragmentation, Mobility, QoS, Aeronautical communications.

1 Introduction

Security in communications can be achieved with a private network that is only accessible by trusted members. However, nowadays traffic between two remote points goes through the public communications infrastructure to avoid the expensive investment needed to deploy a private infrastructure.

A Virtual Private Network (VPN) establishes a private communication over public infrastructure. For that, some protocols like IPsec and TLS/SSL are used. IPsec is a security standard specified by the IETF. It is designed to provide interoperable, high quality, cryptography-based security for IPv4 and IPv6. The set of security services offered includes integrity, authentication, protection against replays, and confidentiality. These services are provided at the IP layer, offering protection for IP and upper layer protocols.

The most common representatives of transport layer security are Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS). TLS/SSL is mainly used on top of TCP, which means that the TCP payload is protected but not the TCP header. The TLS protocol provides security in the form of reliability, integrity, anti-replay and (optionally) confidentiality.

The use of VPNs over satellite links creates additional issues to the ones already present in satellite links, like high delay, bandwidth-delay product and high error rates. These issues and solutions are summarised in the study described on this paper. For example, there are some known solutions like Multi-Layer IPsec to allow the use of transport protocol enhancing proxies inside the IPsec tunnel [1].

P. Pillai, R. Shorey, and E. Ferro (Eds.): PSATS 2012, LNICST 52, pp. 113–118, 2013.

From the satellite operator's point of view, the issues can be seen in three different cases, depending on which nodes it controls along the end-to-end communication path. The feasibility of the technical solutions shall later be then assessed with respect to the constraints posed by these control cases.

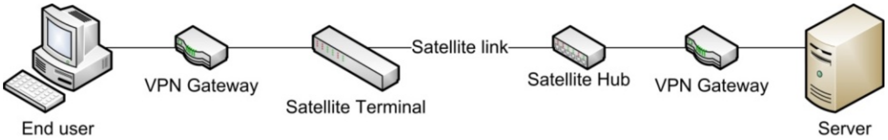

Fig. 1. The communication path as considered for the control cases

Three control cases are defined. Case 1 is when the satellite operator has control over the whole path. In Fig. 1, that corresponds to controlling from one VPN gateway to the other. Case 2 is when there is only control over the satellite related elements; satellite terminal, link and hub in Fig. 1. Case 3 is when, in addition to the satellite elements, one of the VPN gateways is controlled.

This paper starts by explaining the different scenarios considered and further details one of them as an example. Then, the issues of Protocol Enhancing Proxies, IP fragmentation, overhead, mobility, and quality of service are explained. More issues have been identified but are left out due to space limitation.

While the issues and solutions summarised are known, this paper's contribution is the analysis of the applicability of such solutions from the perspective of the satellite operator, according to the different situations represented by the previously defined control cases.

2 Scenarios

Different scenarios have been considered so that it would be possible to investigate: i) the three different control cases, ii) the two security protocols in scope, TLS and IPsec, and later iii) the feasibility of the technical solutions in real-life implementation scenarios. These include:

- ***Public safety.*** It describes de communications between emergency teams deployed on the field and their headquarters.
- ***Aeronautical communications.*** This scenario represents the communications between a mobile network and a static network. In this case, the mobile network is an aeroplane.

The aeronautical scenario is composed of two types of traffic, namely:

- ***Safety-related communications*** consist of communications between pilots and air traffic controllers (Air Traffic Services ATS) and communications between the aircraft and its airline (Airline Operation Control, AOC). The air-to-ground data communication is assumed to be provided by an entity called the Air

Communications Service Provider (ACSP). Because the satellite operator has some influence over the ASCP, this communication path is considered as having control case 1. The traffic in this path is mainly made of short messages, and it uses IPv6 taking into account the recent development in future air traffic management systems [2].

- ***Non safety-related communications*** consists of the traffic that comes from the passengers connecting to the internet (Airline Passenger Communications, APC) and forms the non-safety communications. Because there is no control at the ends of the communication (passenger and the internet) this is a case 2. IPv4 is considered in this path as it is still the most widely used protocol in the Internet.

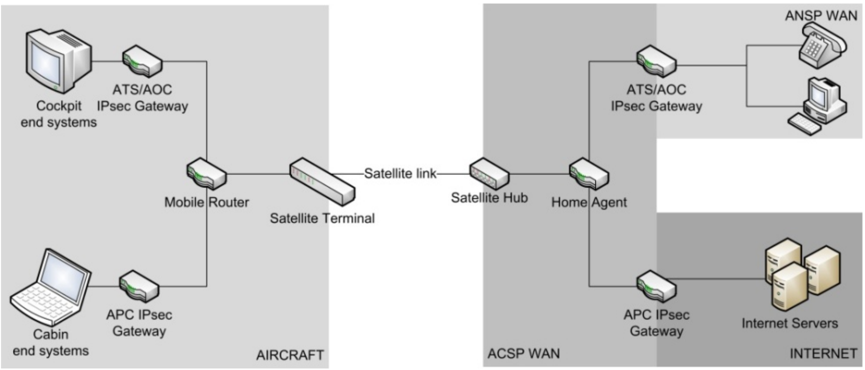

Fig. 2. Aeronautical communications scenario

3 Investigated Technical Issues

3.1 Protocol Enhancing Proxies (PEP)

Standard TCP might not work efficiently in satellite networks due to the bandwidth-delay product and the high bit error rate [3]. PEPs or enhanced TCP are usually used to improve the performance in such networks.

An enhanced version of a protocol differs from the standard protocol in the configuration of some parameters or behaviours (e.g. congestion control mechanism); it is a substitute for the original protocol. On the other hand, PEPs are new elements in the topology configuration that improve the performance of the protocol.

Some PEPs generate TCP packets as if they were the end hosts. Therefore, they must be capable of reading the fields in the TCP header. However, with IPsec these might be encrypted. Even if null encryption is used, after the PEP would generate a new packet, it would be unable to perform IPsec integrity protection and so, the new packet would be dropped at the IPsec gateways. Therefore, the PEPs should be placed outside the IPsec tunnel, requiring a control case 1 when an IPsec VPN is deployed. Some other solutions have been investigated like Multi-Layer IPsec. However, these solutions also require control case 1 and therefore the additional benefits of implementing such solutions are not significant. In the aeronautical communications scenario, due to the short-messages characteristics of the safety communication a gain in performance can be achieved when enhanced TCP, optimised for short messages is used. This is feasible to implement as it represents a control case 1, *and* recommendations by the satellite operator to the end user is possible. In the non-safety communication PEP could be implemented outside the IPsec channel between the airborne and ground APC IPsec GWs, but if the passenger's traffic is already IPsec-protected, the PEP will not bring any improvement.

3.2 Fragmentation

All VPN technologies add some overhead which might increase the packet size beyond the Path Maximum Transfer Unit (PMTU) value of one link in the end-to-end path. Therefore, after deploying a VPN the chances of fragmentation being required are higher. Fragmentation and reassembly are cumbersome. When reassembling, the node needs to wait for all fragments to be received. Fragmentation also adds some overhead, for each fragment requires its own IP header. Also, when happening at routers, they take more time and resources than simple forwarding, effectively increasing the computational load and the delay.

The situation is especially critical if fragmentation happens at the VPN gateway after packets are encapsulated. If that is the case, the receiving VPN gateway is forced to reassemble the packet before decapsulating it, rather than decapsulating each fragment and then forwarding them. This increases the computational load of a single node, the VPN gateway.

There are two proposed solutions. Whenever possible and feasible, the satellite link MTU should be configured to be greater than or equal to the packet sizes generated by both end host plus the VPN overhead. This assures that the packet does not require fragmentation at the satellite link. This solution requires control case 1, since it is required to know the MTU and the traffic characteristics of the end hosts.

Another solution is to use Path MTU Discovery [4]. That is, fragmentation is allowed only at the end hosts, but not at intermediate router.. This is the default behaviour for IPv6 and in IPv4 it is achieved by setting the Don't Fragment (DF) field in the IP header. Packets that exceed the MTU after being processed by the VPN should be dropped. The VPN GW then sends an ICMP message, indicating the path MTU (PMTU), back to the source so it can adapt the size of the packets to fit the tunnel MTU. When using IPv4, this solution requires control case 1.

In the aeronautical scenario, the safety communication uses IPv6 and PMTUD is used by default. In the non-safety communication, PMTUD is enforced at the APC IPsec gateway, by setting the DF bit of all egress IPv4 packets, so that it is dropped in case IPsec causes the packet size to be larger than the link MTU.

3.3 Overhead

VPNs add new headers, causing overhead, which increases the traffic load. However, the impact of this overhead will depend on the payload size. For smaller payloads (like VoIP) the relative increase will be important. For larger payloads the problem is not as bad, but it is still present.

To minimise the effect of such issue, it is proposed to apply header compression to to reduce the overhead. RObust Header Compression (ROHC) has been selected because it is currently the state of the art of header compression protocol that provides high compression efficiency and robustness [5].

This solution will be applied on the satellite link hop since it is the critical link on the path. ROHC can be used to compress ESP or AH headers of IPsec-protected packets. Even though ROHC can also be used to compress the TCP header of TLS-protected packets, the relative compression gain obtained is not significant, as the payload is usually already quite large (TCP will try to create packets with the size up to its maximum segment size (MSS), which takes into account the link MTU). For TLS it is recommended to use TLS-compression, which is part of the TLS specification [6]. ROHC is implemented in the satellite link for both VPN types, so it only requires control case 2.

3.4 Mobility

If at least one of the VPN peers is placed inside a mobile network, then some mobility related issues may appear. For a VPN connection, a handover becomes critical in case the IP address of one VPN peer changes since VPN security associations depend on IP addresses. This is the case for gateway, satellite and gap-filler (technology) handovers. If no mobility features are deployed, the VPN connection will become unusable and a new one has to be setup, requiring maybe a new user interaction for authentication (depends on the authentication mechanism), expensive calculations, and extra round-trips. This is especially critical for satellite links since they have a high round-trip time.

Some solutions have been proposed. One of them is MOBIKE which allows an IPsec security association to accept more than one IP address. The other, Mobile IP consists on giving the mobile node a static IP address (Home Address, HoA) additionally to the IP address given by the network it is plugged in (Care-of-Address, CoA). All packets sent to the HoA are routed through a static node called Home Agent, which knows at all times what CoA corresponds to each HoA. Mobile IP is extended from having a single mobile node to a mobile network with NEMO.

NEMO is the chosen solution for the aeronautical scenario. It is transparent to the end hosts and it is implemented in the satellite link, so it can be implemented even for control case 2. Therefore, it is useful for both safety and non-safety communications. MOBIKE's drawbacks, like being forced to start the communication on the airborne side, discard it as a viable option.

3.5 Quality of Service (QoS)

QoS provisions in the Internet are achieved through IntServ and DiffServ protocols [7] [8]. In both cases, the IP header is used to determine what treatment a datagram receives. Therefore, an IPsec VPNs in tunnel mode will be a problem because it is likely to encrypt the original IP header. A TLS VPNs will not be an issue as it does not protect the network layer.

To still being able to apply QoS at the satellite link (inside the IPsec tunnel), the required information should be present in the outer IP header. This is easily done when using DiffServ, as only the DS field is required, and it should be copied to the outer header according to the IPsec RFC [9]. IntServ access to other fields like source and destination addresses that are not available if the packets are tunnelled using IPsec. It requires control case 1 to assure that the IPsec implementation used at the gateway copies the value and so it can only be assured for the safety communications.

4 Conclusions

In this paper we explained the issues created when deploying a VPN in broadband satellite systems and more specifically, when the satellite links an airplane with the ground.

In case there is no control or influence over the elements in the communication, some of these issues remain untreatable, but for some others, a solution is still applicable. If all the elements are under control, there is at least one solution for each issue. While some solutions, like copying the DSCP value for the QoS issue eliminate the problem, some like header compression only minimise its effects.

Future work involves measuring the performance gains obtained from using the proposed solutions. For that, a testbed integrating the different elements of the aeronautical scenario and the solutions has been set up.

Acknowledgements. This has been conducted in the framework of ESA project "Security in broadband satellite systems for commercial and institutional applications". All fruitful discussions with the project partners and ESA are gratefully acknowledged. This paper does not implicitly represent the opinion of all project partners. The authors are solely responsible for it and do not represent the opinion of the ESA. ESA is not responsible for the use of any data in the paper.

References

1. Zhang, Y.: Multi-Layer Protection Scheme for IPsec. Internet Draft (October 1999)
2. SANDRA project, `http://www.sandra.aero`
3. Border, J., Kojo, M., Griner, J., Montenegro, G., Shelby, Z.: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations. RFC 3135 (June 2001)
4. Mogul, J., Deering, S.: Path MTU Discovery. RFC 1191 (November 1990)
5. Bormann, C., et al.: RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed. RFC 3095 (July 2001)
6. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (August 2008)
7. Braden, R., Clark, D., Shenker, S.: Integrated Services in the Internet Architecture: an Overview. RFC 1633 (June 1994)
8. Blake, S., et al.: An architecture for Differentiated Services. RFC 2475 (December 1998)
9. Kent, S., Seo, K.: Security Architecture for the Internet Protocl. RFC 4301 (December 2005)