

Recommendations on using VPN over SATCOM

Romain Guilloteau
VIVERIS TECHNOLOGIES

David Pradas
VIVERIS TECHNOLOGIES

Guillaume Pelat
VIVERIS TECHNOLOGIES

Nicolas Kuhn
CNES

Abstract—VPN are a secured tunnel that help service providers to exchange data over non-secured networks. There is a large variety of VPN solutions that have variable deployment impacts on the target architecture as well as performance limitations or opportunities.

This technical report compares Wireguard and OpenVPN for various SATCOM deployment scenarios and topologies.

Index Terms—VPN, SATCOM, PEP, TCP

I. INTRODUCTION

Working from home or interconnecting enterprise networks increase security needs, and this can be fulfilled by taking advantage of VPN solutions. When using HTTPS is not enough, an added layer of security may be deployed to guarantee that crossing a non-secured network will be safe.

Since VPN can operate at the application or network layer, comparing VPN solutions may not be straightforward. Wireguard [1] operates at the network layer and aims at replacing IPsec for most use cases. OpenVPN [2] works at the application layer and is not compatible with IPsec.

Depending on the scenarios of deployment, it may not be easy for an IT system provider to guarantee end-to-end performances for one solution or the other one. As an example, Wireguard operating at the kernel level depends on the machine on which it is deployed, while OpenVPN can be tuned to the deployment use case by, e.g. using TCP or UDP to carry the secured tunnel traffic.

SATCOM systems exhibit a wide variety, both in terms of delay and goodput, making it hard to assess the relevant VPN solution for a specific scenario [3]. Indeed, for the sake of good end-to-end performance, SATCOM systems deploy Performance Enhancing Proxies [4]. Exploiting VPN tunnels may result in by-passing these proxies and impact the goodput of data transfers.

This technical report contributes to the performance evaluation of VPN tunnels. We do not claim to provide the most extensive study on the subject, since we focus on the SATCOM scenarios. That being said, the performance evaluation may be of interest for other scenarios where performance enhancing proxies are deployed.

II. SCENARIOS

This section describes the scenario that has been considered throughout this evaluation study. It also presents the SATCOM system and the characteristics of the VPN solutions.

A. Architecture

The architecture that will be exploited in this technical report is reported in Figure 1.

An end user (PC) is connected to a box (offering Internet/media services and satellite access management) that includes the VPN client. A satellite terminal, a satellite and a satellite gateway interconnect the client's box to a POP (Point of Presence) that includes the VPN server. Then, the POP is connected to the enterprise LAN that contains the server that the end user aims to reach.

The SATCOM solution might integrate a performance enhancing proxy that may be either within or out of the VPN tunnel.

B. SATCOM system

The satellite system is emulated with `netem` and the tests are orchestrated with OpenBACH [5]. This technical report consider GEO and LEO systems. The characteristics of each system are the following:

- GEO : RTT of 500 ms, bottleneck bandwidth of 10 Mbps
- LEO : variable RTT, bottleneck bandwidth of 10 Mbps

End-to-end losses on SATCOM systems have been measured in [6]. In order to assess the impact of losses on the proposed solutions, we have also included random losses on the SATCOM system.

The PEP has been configured with the following options:

- Before or after the VPN tunnel
- CUBIC, CUBIC without Hystart and BBRv2
- Various initial congestion windows

C. VPN solutions

The VPN solutions are either Wireguard or OpenVPN. In particular, the following parameters have been configured for OpenVPN:

- Adapted socket buffer sizes (to match the Bandwidth-Delay-Product of the network)
- MTU/MSS size
- UDP or TCP mode

D. Application layer

The following end-to-end applications have been introduced:

- File transfers with `iperf3`
- Web transfers
- VoIP

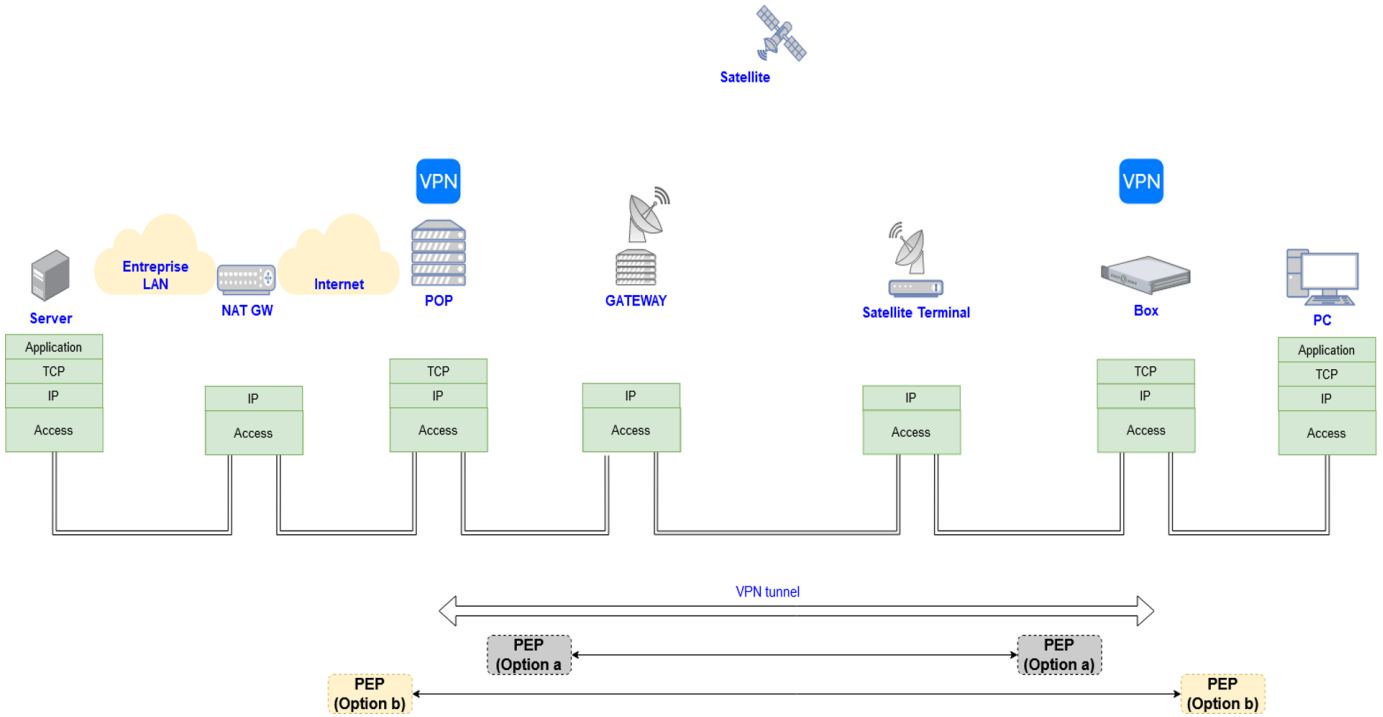


Fig. 1. Platform architecture

III. SINGLE FLOW SCENARIOS

This section includes the results that have been obtained. A subset of the obtained results is presented and more results, based on the parameters listed in Section II, are available upon request.

This section presents the results for a 30 MB file transfer when only one flow is considered. The options are the following:

- VPN : no VPN, OpenVPN (UDP and TCP) and Wireguard;
- PEP : no PEP, PEP in B position or PEP in A position;
- Transport (applied end-to-end and on the PEP): CUBIC (with or without Hystart) or BBRv2.

The results are shown in Figure 2. The table gathers all the results. Comparative tables are shown in Figure 3, Figure 4, Figure 5 and Figure 6.

A. No loss scenarios

The results are shown in Figure 2, Figure 3 and Figure 4.

All transport layer variants are affected by the presence of a VPN, but the difference can be neglected.

When a VPN has to be included, the solution based on OpenVPN TCP in PEP position A results in the worst performance (i.e. "TCP in TCP" issue) by increasing the transfer time by at least 10 %.

When a VPN has to be included, it is then recommended to use Wireguard with a PEP in position B. It is worth mentioning that other configurations, such as OpenVPN UDP with/without PEP and Wireguard without PEP, exhibit fair performance. Indeed, when we do not consider the OpenVPN

TCP in PEP position A configuration, the time to transfer is further reduced by only up to 5 % with Wireguard with PEP in position B if compared with the one achieved with aforementioned configurations.

B. Loss scenarios

The results are shown in Figure 2, Figure 5 and Figure 6.

When there are losses on the satellite link, the choice of BBRv2 as a transport layer protocol helps in improving well-known TCP CUBIC issues when lossy links are considered. In this case, OpenVPN UDP or Wireguard show the best performances specially for GEO satellites. However, there are cases where the end-to-end congestion control can not be adapted (e.g. with end-to-end QUIC flows or end servers non-managed by the operator).

In the case where the end-to-end transport is CUBIC, OpenVPN TCP exhibits the best performance by reducing the transfer time by 30% as opposed to the case where no VPN and no PEP is proposed for the LEO scenario. In the case where the end-to-end transport is CUBIC, for the GEO scenario, OpenVPN TCP also exhibits the best configuration.

The recommendations that are proposed in this section are mainly related to the position of the losses. They are currently emulated in the satellite link and other position (e.g. losses on the LAN link) may differ. In particular, the gains brought by PEP when losses are located at the last-mile would be more important.

IV. MULTIPLE FLOW SCENARIOS

This document reported so far results on the single flow scenarios and on the scenarios where the congestion controls

No loss LEO								
VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
PEP	None	None	A	B	None	B	None	B
CUBIC w/o Hystart	26,8	29,8	29,9	29,5	28,9	28,7	28,3	28,0
CUBIC w Hystart	27,1	29,6	32,0	29,3	28,9	28,6	28,4	28,0
BBRv2	27,9	30,8	31,6	30,3	29,7	29,2	29,2	28,7

Loss LEO								
VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
PEP	None	None	A	B	None	B	None	B
CUBIC w/o Hystart	244,7	181,4	179,2	190,1	347,2	249,1	336,1	242,3
CUBIC w Hystart	231,8	184,7	174,8	184,9	352,7	255,6	339,8	249,9
BBRv2	32,6	32,8	33,3	34,9	31,7	34,0	32,2	34,0

No Loss GEO								
VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
PEP	None	None	A	B	None	B	None	B
CUBIC w/o Hystart	29,4	33,7	34,2	34,4	31,7	31,0	30,9	30,4
CUBIC w Hystart	29,9	34,5	38,6	34,1	31,4	31,0	33,0	30,5
BBRv2	32,8	35,7	39,8	35,4	33,9	33,4	33,4	32,2

Loss GEO								
VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
PEP	None	None	A	B	None	B	None	B
CUBIC w/o Hystart	358,4	380,0	339,0	334,9	508,1	507,1	529,8	521,1
CUBIC w Hystart	326,2	357,5	334,3	346,0	518,4	484,9	524,0	498,3
BBRv2	35,9	50,7	49,3	49,1	38,1	37,7	37,0	36,4

Fig. 2. Summary of the results - 30 MB file transfer time (s)

where the same on all entities. In the framework of this study, experiments with multiple flows and with congestion controls that are different on the end host and on the PEP have been also done. This section sums up the main conclusions of this extended activity and the details may be provided up-on request.

A. CUBIC on the end hosts and BBRv2 on the PEP

In order to have more confidence on the recommendation on exploiting BBRv2 whenever it can be applied, it can be noted that the experiments considered BBRv2 on the end hosts and on the PEP. As a result, we can hardly guarantee that the conclusions would be the same if BBRv2 was applied only on the PEP, while CUBIC is applied on the end host. We have compared the downloading time of a 30 MB file in the case where BBRv2 is applied on all entities and in the case where BBRv2 is applied everywhere but the end host.

The only case where the performance are not acceptable is the one where CUBIC is applied end-to-end and the PEP could not split the traffic (and apply BBRv2 on the lossy segment of the network). When the connection can be split, the gains brought by BBRv2 tolerance to packet loss are present: the transfer time oscillates between 32 and 46 seconds.

As a result, when BBRv2 can be exploited on the lossy segments, using it whenever possible remains the recommendation of this paper.

B. Impact of using multiple flows

To assess the impact of using multiple flows across the network, we have considered:

- for the loss-less scenarios: a flow that transmits data during hundred seconds and a second flow starting ten seconds later that transmits data during eighty seconds.
- for the loss scenarios: a flow that start an unlimited data transfer and a second flow transmit thirty MB ten seconds later.

In the loss-less scenarios, Wireguard with a PEP in a B position enabled the largest amount of data transmitted in general and did not increase considerably the unfairness between the two flows. In all configurations of PEP and VPN, the capacity sharing between the flows oscillates between 40 % and 60 %.

In the loss scenarios, Wireguard also exhibited the best performance in terms of 30 MB transfer time and did not impact the existing unfairness between the two flows that were considered.

OpenVPN TCP did not exhibit good performance in the multiple flow scenarios, which may resides in the fact that multiple TCP flows are tunneled within one single TCP flow. As a result, when using OpenVPN TCP, it is recommended to consider one tunnel per TCP flow.

REFERENCES

- [1] "Wireguard," <https://www.wireguard.com/>.
- [2] "OpenVPN," <https://openvpn.net/>.
- [3] T. Jones, G. Fairhurst, N. Kuhn, J. Border, and S. Emile, "Enhancing transport protocols over satellite networks," Working Draft, IETF Secretariat, Internet-Draft draft-jones-tsvwg-transport-for-satellite-00, February 2021, <https://www.ietf.org/archive/id/draft-jones-tsvwg-transport-for-satellite-00.txt>.

No loss LEO		VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
CUBIC w/o Hystart		PEP	None	None	A	B	None	B	None	B
VPN	PEP									
None	None			-11%	-11%	-10%	-8%	-7%	-6%	-5%
OpenVPN TCP	None		10%		0%	1%	3%	4%	5%	6%
	A		10%	0%		1%	3%	4%	5%	6%
	B		9%	-1%	-1%		2%	3%	4%	5%
OpenVPN UDP	None		7%	-3%	-3%	-2%		1%	2%	3%
	B		7%	-4%	-4%	-3%	-1%		1%	2%
Wireguard	None		5%	-5%	-6%	-4%	-2%	-1%		1%
	B		4%	-6%	-7%	-5%	-3%	-2%	-1%	

No loss LEO		VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
CUBIC w Hystart		PEP	None	None	A	B	None	B	None	B
VPN	PEP									
None	None			-9%	-18%	-8%	-7%	-6%	-5%	-3%
OpenVPN TCP	None		8%		-8%	1%	2%	3%	4%	5%
	A		15%	7%		8%	10%	11%	11%	12%
	B		8%	-1%	-9%		1%	2%	3%	4%
OpenVPN UDP	None		6%	-3%	-11%	-1%		1%	2%	3%
	B		5%	-4%	-12%	-2%	-1%		1%	2%
Wireguard	None		5%	-4%	-13%	-3%	-2%	-1%		1%
	B		3%	-6%	-14%	-5%	-3%	-2%	-1%	

No loss LEO		VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
BBRv2		PEP	None	None	A	B	None	B	None	B
VPN	PEP									
None	None			-10%	-13%	-8%	-6%	-5%	-4%	-3%
OpenVPN TCP	None		9%		-3%	2%	4%	5%	5%	7%
	A		12%	3%		4%	6%	8%	8%	9%
	B		8%	-2%	-5%		2%	4%	4%	5%
OpenVPN UDP	None		6%	-4%	-6%	-2%		2%	2%	4%
	B		4%	-6%	-8%	-4%	-2%		0%	2%
Wireguard	None		4%	-6%	-8%	-4%	-2%	0%		2%
	B		2%	-8%	-10%	-6%	-4%	-2%	-2%	

Fig. 3. Comparative results - No loss LEO scenario

- [Online]. Available: <https://www.ietf.org/archive/id/draft-jones-tsvwg-transport-for-satellite-00.txt>
- [4] J. Border and M. Kojo and J. Griner and G. Montenegro and Z. Shelby, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations," Internet Requests for Comments, RFC Editor, RFC 3135, June 2001.
- [5] "OpenBACH," <https://www.openbach.org/>.
- [6] N. Kuhn, F. Michel, L. Thomas, E. Dubois, and E. Lochin, "Quic: Opportunities and threats in satcom," in *2020 10th Advanced Satellite Multimedia Systems Conference and the 16th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, 2020, pp. 1–7.

No loss GEO CUBIC w/o Hystart		VPN	None	OpenVPN TCP		OpenVPN UDP		Wireguard		
VPN	PEP	PEP	None	None	A	B	None	B	None	B
None	None			-15%	-16%	-17%	-8%	-5%	-5%	-3%
OpenVPN TCP	None		13%		-2%	-2%	6%	8%	8%	10%
	A		14%	1%		0%	7%	9%	10%	11%
	B		14%	2%	0%		8%	10%	10%	11%
OpenVPN UDP	None		7%	-6%	-8%	-8%		2%	3%	4%
	B		5%	-9%	-10%	-11%	-2%		0%	2%
Wireguard	None		5%	-9%	-11%	-11%	-3%	0%		1%
	B		3%	-11%	-12%	-13%	-4%	-2%	-2%	

No loss GEO CUBIC w Hystart		VPN	None	OpenVPN TCP		OpenVPN UDP		Wireguard		
VPN	PEP	PEP	None	None	A	B	None	B	None	B
None	None			-15%	-29%	-14%	-5%	-4%	-10%	-2%
OpenVPN TCP	None		13%		-12%	1%	9%	10%	4%	12%
	A		22%	10%		11%	19%	20%	14%	21%
	B		12%	-1%	-13%		8%	9%	3%	11%
OpenVPN UDP	None		5%	-10%	-23%	-9%		1%	-5%	3%
	B		3%	-11%	-24%	-10%	-1%		-7%	2%
Wireguard	None		9%	-5%	-17%	-3%	5%	6%		8%
	B		2%	-13%	-26%	-12%	-3%	-2%	-8%	

No loss GEO BBRv2		VPN	None	OpenVPN TCP		OpenVPN UDP		Wireguard		
VPN	PEP	PEP	None	None	A	B	None	B	None	B
None	None			-9%	-21%	-8%	-3%	-2%	-2%	2%
OpenVPN TCP	None		8%		-11%	1%	5%	7%	7%	10%
	A		18%	10%		11%	15%	16%	16%	19%
	B		7%	-1%	-13%		4%	6%	6%	9%
OpenVPN UDP	None		3%	-5%	-17%	-4%		2%	2%	5%
	B		2%	-7%	-19%	-6%	-2%		0%	4%
Wireguard	None		2%	-7%	-19%	-6%	-2%	0%		4%
	B		-2%	-11%	-24%	-10%	-5%	-4%	-4%	

Fig. 4. Comparative results - No loss GEO scenario

Loss LEO CUBIC w/o Hystart		VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
VPN	PEP	PEP	None	A	B	None	B	None	B	
None	None		26%	27%	22%	-42%	-2%	-37%	1%	
OpenVPN TCP	None		-35%	1%	-5%	-91%	-37%	-85%	-34%	
	A		-37%	-1%	-6%	-94%	-39%	-88%	-35%	
	B		-29%	6%		-83%	-31%	-77%	-27%	
OpenVPN UDP	None		30%	48%	45%		28%	3%	30%	
	B		2%	27%	24%	-39%		-35%	3%	
Wireguard	None		27%	46%	43%	-3%	26%		28%	
	B		-1%	26%	22%	-43%	-3%	-39%		

Loss LEO CUBIC w Hystart		VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
VPN	PEP	PEP	None	A	B	None	B	None	B	
None	None		20%	25%	20%	-52%	-10%	-47%	-8%	
OpenVPN TCP	None		-25%	5%	0%	-91%	-38%	-84%	-35%	
	A		-33%	-6%	-6%	-102%	-46%	-94%	-43%	
	B		-25%	0%	5%	-91%	-38%	-84%	-35%	
OpenVPN UDP	None		34%	48%	50%		28%	4%	29%	
	B		9%	28%	28%	-38%		-33%	2%	
Wireguard	None		32%	46%	46%	-4%	25%		26%	
	B		7%	26%	26%	-41%	-2%	-36%		

Loss LEO BBRv2		VPN	None	OpenVPN TCP			OpenVPN UDP		Wireguard	
VPN	PEP	PEP	None	A	B	None	B	None	B	
None	None		0%	-2%	-7%	3%	-4%	1%	-4%	
OpenVPN TCP	None		0%	-2%	-7%	3%	-4%	2%	-4%	
	A		2%	2%	-5%	5%	-2%	3%	-2%	
	B		7%	6%	5%	9%	3%	8%	3%	
OpenVPN UDP	None		-3%	-3%	-10%		-7%	-1%	-7%	
	B		4%	4%	-3%	7%		5%	0%	
Wireguard	None		-1%	-3%	-9%	1%	-6%		-6%	
	B		4%	4%	2%	7%	0%	5%		

Fig. 5. Comparative results - Loss LEO scenario

Loss GEO		VPN	None	OpenVPN TCP		OpenVPN UDP		Wireguard		
CUBIC w/o Hystart		PEP	None	None	A	B	None	B	None	B
VPN	PEP									
None	None			-6%	5%	7%	-42%	-42%	-48%	-45%
OpenVPN TCP	None		6%		11%	12%	-34%	-33%	-39%	-37%
	A		-6%	-12%		1%	-50%	-50%	-56%	-54%
OpenVPN UDP	B		-7%	-13%	-1%		-52%	-51%	-58%	-56%
	None		29%	25%	33%	34%		0%	-4%	-3%
Wireguard	B		29%	25%	33%	34%	0%		-4%	-3%
	None		32%	28%	36%	37%	4%	4%		2%
Wireguard	B		31%	27%	35%	36%	2%	3%	-2%	

Loss GEO		VPN	None	OpenVPN TCP		OpenVPN UDP		Wireguard		
CUBIC w Hystart		PEP	None	None	A	B	None	B	None	B
VPN	PEP									
None	None			-10%	-2%	-6%	-59%	-49%	-61%	-53%
OpenVPN TCP	None		9%		6%	3%	-45%	-36%	-47%	-39%
	A		2%	-7%		-3%	-55%	-45%	-57%	-49%
OpenVPN UDP	B		6%	-3%	3%		-50%	-40%	-51%	-44%
	None		37%	31%	36%	33%		6%	-1%	4%
Wireguard	B		33%	26%	31%	29%	-7%		-8%	-3%
	None		38%	32%	36%	34%	1%	7%		5%
Wireguard	B		35%	28%	33%	31%	-4%	3%	-5%	

Loss GEO		VPN	None	OpenVPN TCP		OpenVPN UDP		Wireguard		
BBRv2		PEP	None	None	A	B	None	B	None	B
VPN	PEP									
None	None			-41%	-37%	-37%	-6%	-5%	-3%	-1%
OpenVPN TCP	None		29%		3%	3%	25%	25%	27%	28%
	A		27%	-3%		0%	23%	23%	25%	26%
OpenVPN UDP	B		27%	-3%	0%		22%	23%	25%	26%
	None		6%	-33%	-29%	-29%		1%	3%	5%
Wireguard	B		5%	-34%	-31%	-30%	-1%		2%	4%
	None		3%	-37%	-33%	-33%	-3%	-2%		2%
Wireguard	B		1%	-39%	-35%	-35%	-5%	-4%	-2%	

Fig. 6. Comparative results - Loss GEO scenario