Recommendations on using VPN over SATCOM access

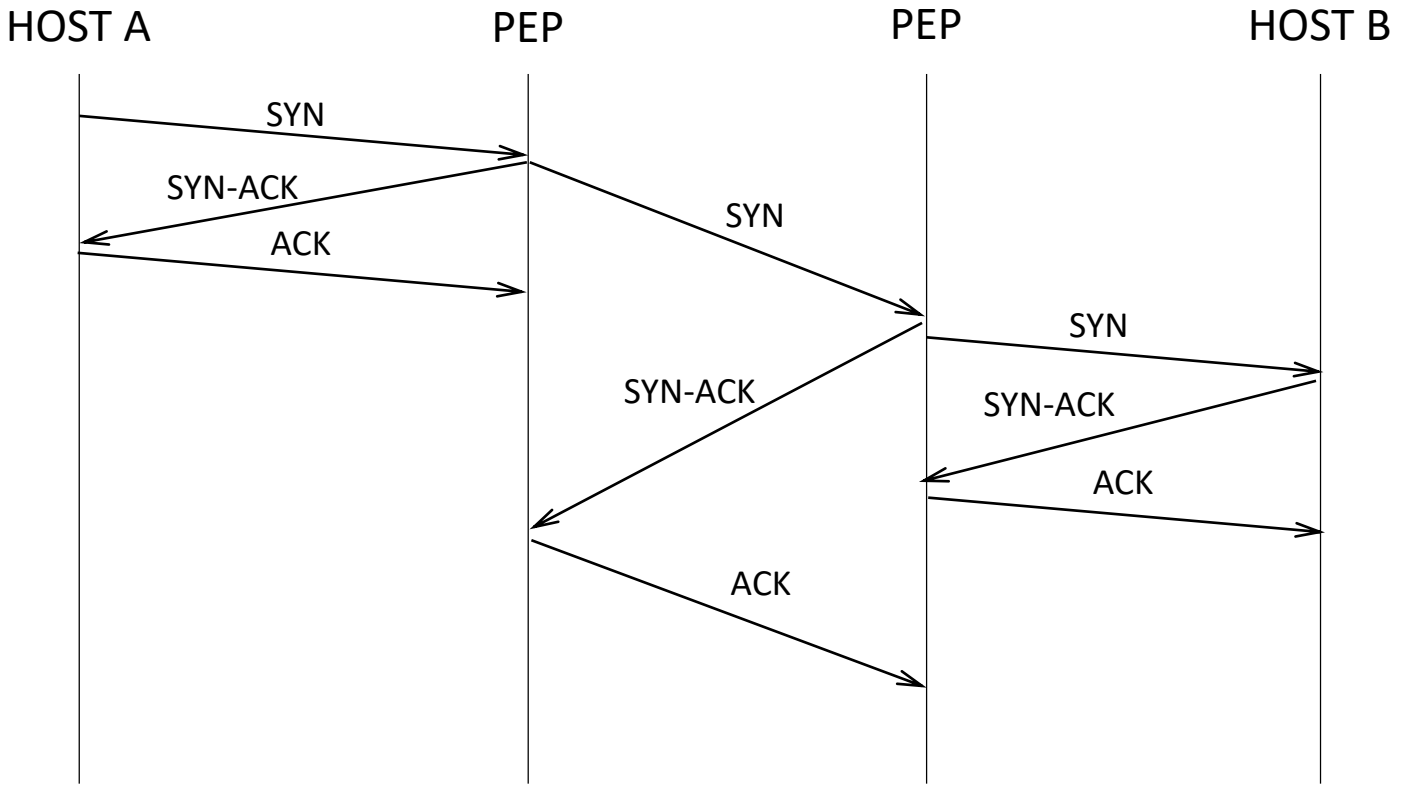
David PRADAS (VIVERIS)
Romain Guilloteau (VIVERIS TECHNOLOGIES)
Guillaume Pelat (VIVERIS TECHNOLOGIES)
Nicolas Kuhn (CNES)

VPN are everywhere

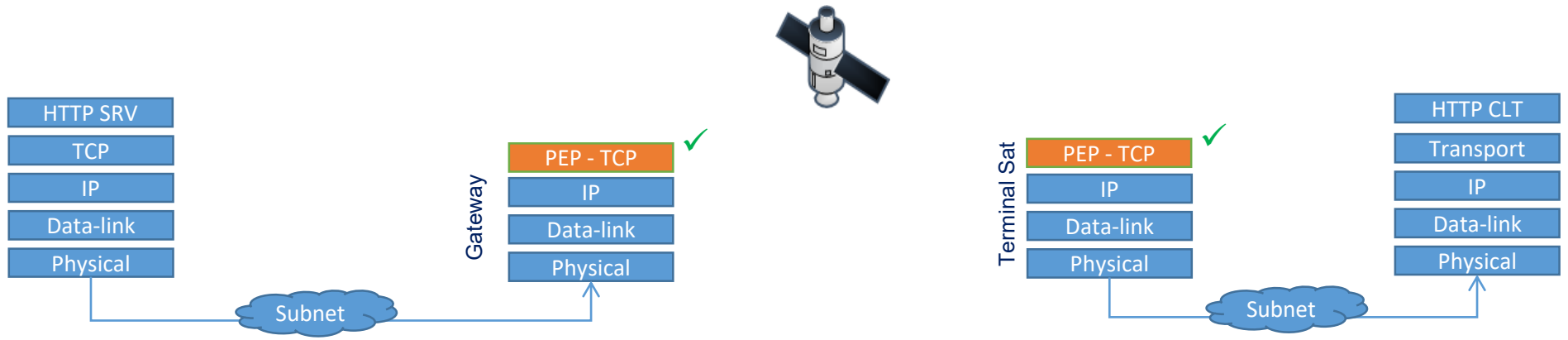
- Working from home, interconnecting entreprise networks
  - ➢increase security needs
  - ➢VPN helps !
- Using HTTPS may not be enough
  - ➢added layer of security
  - ➢crossing a non-secured network will be safe
- Lots of VPN solutions and configurations
  - Wireguard (IPSec)
  - OpenVPN (OpenSSL, SSL, TLS) on top of UDP or TCP

TCP-splitting middleboxes are everywhere too! (and in particular in SATCOM systems)

- SATCOM systems typically deploy TCP Proxy (PEP) [RFC3135]

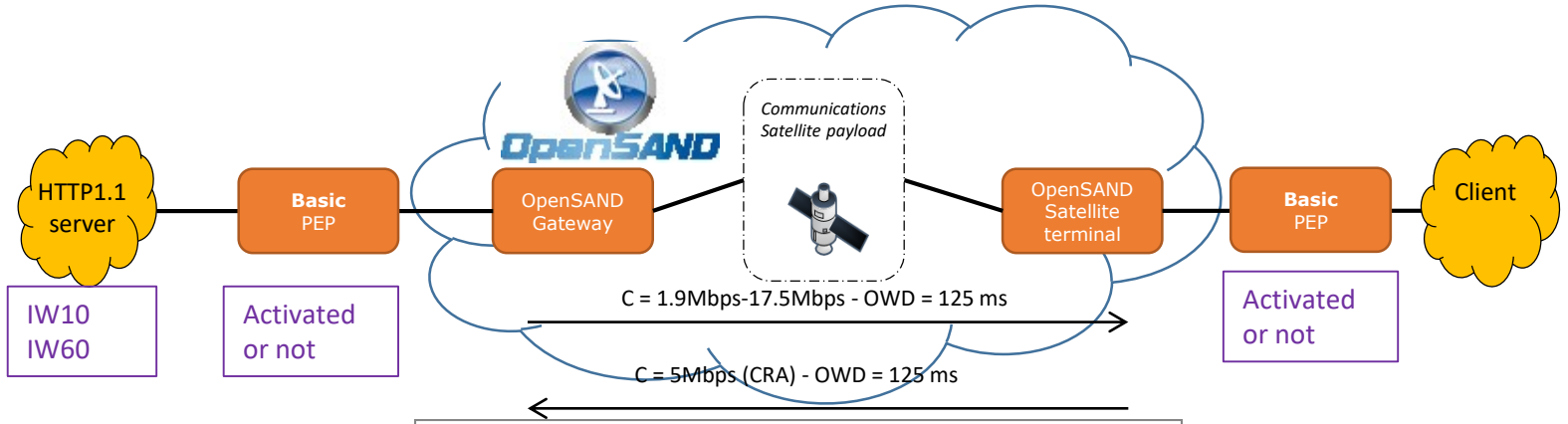


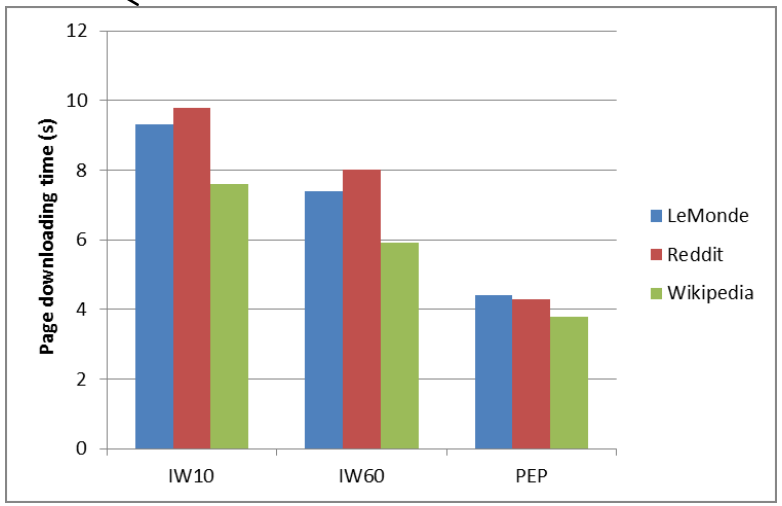
TCP-splitting middleboxes are everywhere too! (and in particular in SATCOM systems)



- Connection initialization:
  - setting up the connection requires three round trips, impacting the moment from which the actual data can be transmitted
  - ➢ Improved by custom TCP initial windows in TCP - PEP
- Window size required:
  - to fully exploit the available capacity, it is necessary to increase the sending buffers are the client and the server
  - ➢ Improved by custom TCP buffers in TCP - PEP
- Reliability:
  - packet loss detection and correction is slow (end-to-end retransmission performance is also affected on GEO access)
  - ➢ Loss recovery in splitted in three segments
- Convergence of congestion control:
  - the exponential increase in data rate is considerably slowed down for a GEO satellite.
  - ➢ Improved by custom TCP AIMD in TCP - PEP

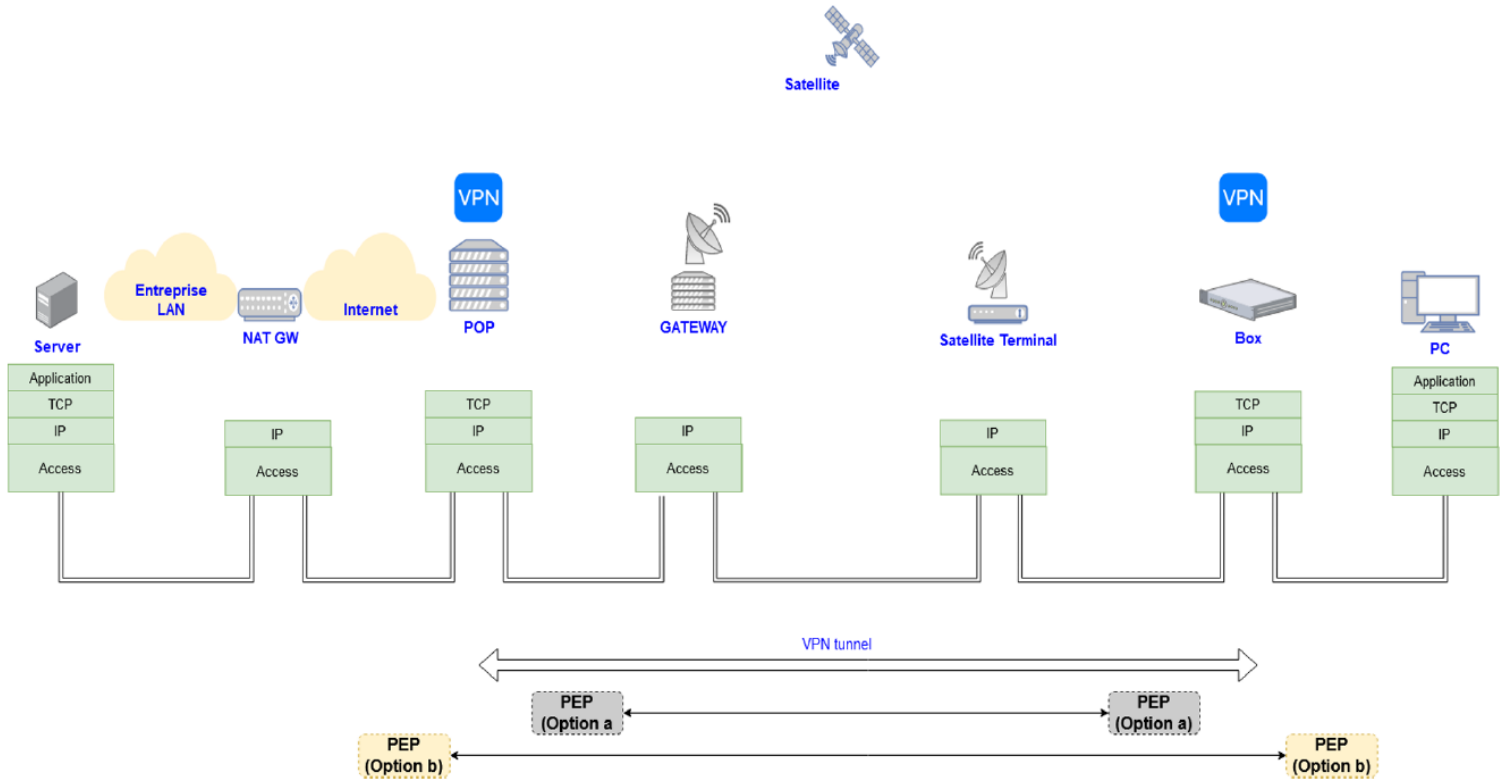
TCP-splitting middleboxes are everywhere too! (and in particular in SATCOM systems)





Rationale of the study

- I have VPN and PEP … do they cooperate ?
- What VPN should I use ?
- If I can choose my congestion control … what should it be ?



Configurations

- SATCOM
  - GEO : RTT of 500 ms, bottleneck bandwidth of 10 Mbps
  - LEO : variable RTT, botteleneck bandwidth of 10 Mbps
  - Random losses on the SATCOM link
- PEP
  - Before (Option B) or after (Option A) the VPN tunnel
  - CUBIC, CUBIC without Hystart and BBRv2
  - Various initial congestion windows
- Same congestion control applied to all the nodes
- VPN
  - Wireguard
  - OpenVPN UDP
  - OpenVPN TCP
- Application : 30MB file transfer

Results – no loss scenario

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

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

- OpenVPN TCP in PEP position A: worst performance (i.e. ”TCP in TCP” issue)
- Wireguard with a PEP in position B : best performance
- OpenVPN UDP with/without PEP and Wireguard without PEP : fair performance

Results – loss scenario

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

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

- Losses on the satellite link : BBRv2 as a transport layer protocol helps
- When the end-to-end congestion control can not be adapted, when the end-to-end transport is CUBIC
  - OpenVPN TCP exhibits the best performance by reducing the transfer time

Summary

- No loss
  - Use wireguard with a PEP in B position (before the Wireguard instance)
  - CUBIC and BBRv2 exhibit (more or less) the same performance
- With losses
  - BBRv2 helps a lot
  - When BBRv2 is not possible, damages can be reduced with the usage of OpenVPN TCP
- Limits of the conclusion :
  - When losses are on the LAN, PEP can help a lot (split the recovery process)
  - In the study, losses are applied on the long-delay satellite link : PEP can not really help the loss recovery process
- More details on ArXiv paper
  - “Recommendations on using VPN over SATCOM”; David PRADAS, Romain Guilloteau, Guillaume Pelat, Nicolas Kuhn