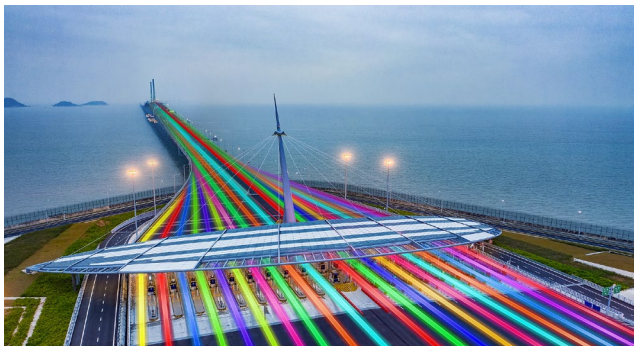
LANCOM Techpaper

LANCOM High Scalability VPN (HSVPN)

In the interest of the secure exchange of sensitive data in networks, the encryption technology IPSec VPN is required for networking corporate offices, branches, home offices, and mobile workers. This involves an encrypted data tunnel being established through the public Internet, which creates a secure private network that provides access only to authorized users. In most cases, a number of logically separate networks (VLANs) need to be provided for different company applications at the different tunnel endpoints—which, for large multi-service IP networks, leads to a complexity that should not be underestimated. Instead of dedicating a separate infrastructure and different Internet connections to each application, we recommend that you use network virtualization. Various methods are used according to the underlying infrastructure, each of which have developed in a kind of "evolution" with different strengths and weaknesses. These are described in this techpaper.



Three methods of multi-site network virtualization

Multi-PPTP-over-IPSec (tunnel-in-tunnel)

Many networking scenarios work with multiple logical networks that are managed in isolation from one another (Advanced Routing & Forwarding, ARF). To achieve a true end-to-end network virtualization via IPSec VPN, an IPSec tunnel that contains further PPTP or L2TP tunnels must be established between the VPN gateways. These tunnels-in-tunnels have to be independent of the IP address ranges of the networks being interconnected. The PPTP and L2TP protocols are long-established tunnel technologies. Similar to VLAN in LAN, a PPTP tunnel is established for each ARF context, and this transmits the corresponding VLANs of the sites separately through an IPSec tunnel (see figure 1). The VLAN information available in layer 2 is used to connect the networks to the individual PPTP tunnels, which in turn are transmitted over the Internet through a shared IPSec VPN tunnel. This makes it possible to completely virtualize the network segments for an entire corporate network.

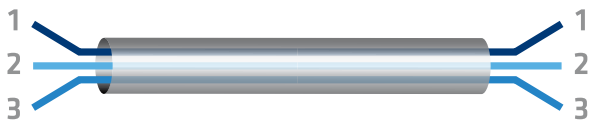


Fig. 1: Multi-PPTP-over-IPSec (tunnel-in-tunnel)

This method uses just one IPSec VPN tunnel to transmit several separate networks. However, this nesting of the tunnels does create a considerable amount of overhead in the data packets. The VPN gateways at each tunnel endpoint have to handle the extra load of packing and unpacking each data packet multiple times, which in turn requires the routing table to be processed more frequently, so increasing the use of computing power still further.

Advantages: You only need as many IPSec tunnels as locations, which reduces the load on the VPN gateways from IPSec negotiations and rekeying.

Disadvantages: Reduced MTU through tunnel-in-tunnel nesting. Inefficient packet transport as each packet has to be packed and unpacked twice.

IPSec per network (multi-VPN)

IPSec VPN is a tried-and-tested, secure method of virtualizing an Internet-based transmission path between two sites. However, IPSec does not offer any options for forwarding logically separated networks (e.g. by VLAN and ARF) through an IPSec tunnel while maintaining the logical separation. To get around this problem, a separate IPSec VPN tunnel can be set up for each IP network (see figure 2).

Fig. 2: IPSec per network (multi-VPN)

This simple architecture requires high CPU performance at both tunnel endpoints, since IPSec negotiation is required for each of the networks. At the same time, the underlying IPSec gateways must be able to support the required number of parallel IPSec VPN tunnels: The number of VPN tunnels to be terminated is the number of networks multiplied by the number of sites.

Advantages: Transmission is highly efficient because the MTU is maximized and packets only have to be packed and unpacked once by the router.

Disadvantages: VPN endpoints are subject to a heavy load from the IPSec negotiations and rekeying. This results in a time-consuming tunnel establishment, both initially and in the event of a failover.

LANCOM High Scalability VPN (HSVPN)

The "IPSec per Network" variant optimizes the throughput, since the "Multi-PPTP-over-IPSec" variant was relatively inefficient in this respect. The focus in that case was on separating the data streams. However, efficient network virtualization by means of IPSec VPN should generally keep the number of tunnels—IPSec or PPTP—to a minimum and make the MTU size as large as possible. This is done in a further optimization step called LANCOM High Scalability VPN (HSVPN), which further reduces the number of IPSec tunnels.

Comparison of the number of tunnels established with the presented methods

- Multi-PPTP-over-IPSec
  Number of sites * Number of ARF * PPTP/L2TP + Number of sites * IPSec
- IPSec per Network
  Number of sites * Number of ARF * IPSec
- LANCOM High Scalability VPN (HSVPN)
  Number of sites * IPSec

It is important to note that the transmission path within the IPSec tunnel and the router is more efficient than with Multi-PPTP-over-IPSec. The individual ESP packets are suffixed with a "trailer", which contains a routing tag in encrypted form. This is similar to how the VLAN tag (IEEE 802.1Q) functions in the Ethernet frame. Marked in this way, logically separated IP data packets can be transmitted in parallel, even without further nested tunnels: The receiving VPN gateway uses the trailer to assign the

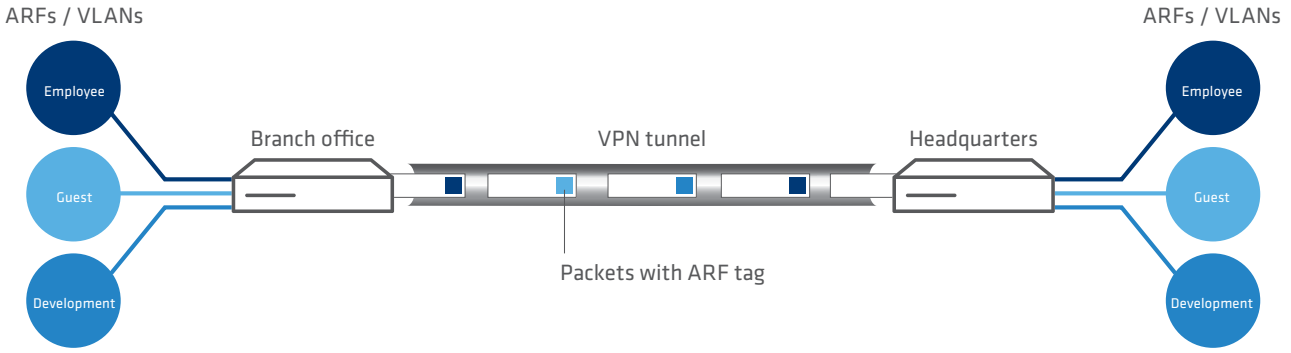


Fig. 3: LANCOM High Scalability VPN (HSVPN)

incoming IP data packet to its ARF context and forwards it to the corresponding destination address (see figure 3).

With regard to the encryption, LANCOM HSVPN is a modern IPSec that is based on standards-compliant IKEv2 and thus offers exactly the same security as IKEv2. Furthermore, it does not depend on central management instances and works as an independent, decentralized system. As with the other methods, there is no change in the necessary encryption performance. Each packet was and is encrypted once only.

Advantages: The load is reduced because only one tunnel is required per site. As a result, fewer tunnels need to be established and managed overall (rekeying). At the same time, less load is required for packet transport as the packets do not have to negotiate several tunnels and do not have to be packed and unpacked multiple times.

Although this procedure is not available between different manufacturers, the technologies used are based on the IPSec standard and thus inherit that method's security. While network separation by means of trailers is just as efficient and secure as separation through an inner tunnel, it incurs significantly lower overhead.

Summary

The more complex a network infrastructure is, the more important is the choice of a suitable network virtualization method during the planning and implementation, in particular with regard to multi-site transmission paths. The basic recommended approach is to use the smallest possible number of data tunnels without foregoing the strict separation of the routing contexts and the security of modern IPSec. This is exactly what LANCOM High Scalability VPN achieves.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions. 01/2020