White paper

Finding the right VPN solution

Sectra Communications

Do your staff need to be online securely with their mobile devices while on the go—at the office, between floors, out in the street, in the car or on a train—without having to connect again and again? If this is the case, your organization probably needs a modern Layer 4 VPN, and not a traditional Layer 3.

Working remotely brings employees greater freedom and flexibility, and new opportunities arise with the potential to work anywhere, any time. The need for a secure mobile workplace is therefore greater than ever. While there are many positive aspects to a mobile workforce, there are many risks to consider as well.

Organizations have a great deal of important and sensitive information they want to protect, of course, but insecure connections while working outside the office entail a higher risk of being targeted by cyberattacks. To keep information secure and to meet the requirements for a secure mobile workplace, organizations need to upgrade to a VPN that has been developed for a mobile world.

A VPN suited for a mobile world

VPN is traditionally designed to facilitate working remotely from one or more stationary points to another—for example, an employee with a laptop who needs to access the company's server from their home office or a hotel room. These were yesterday's challenges, but to some extent they are also today's.

Tomorrow's challenge—also today's—is to facilitate fully mobile work from smartphones and tablets. People work when moving about, for example, in healthcare when staff take their mobile devices with them while going from one department or floor to another. Another example is police and other emergency services that are always on the move and often need access to data and information from the company's server.

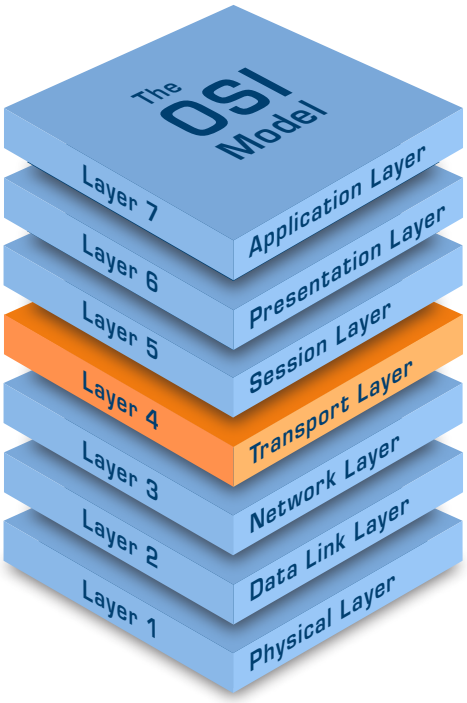
What these examples have in common is that these professions process sensitive information that they always need access to in order to perform their work, while always keeping the information protected through a secure connection.

To secure the connection between the user's client and the company's server, a VPN is applied. VPNs can be designed based on communication taking place on Layer 3, the network layer, in the Open Systems Interconnection model (OSI model), or on Layer 4, the transport layer. OSI is a conceptual model that shows how various computer systems can communicate with one another. In the following section, we will look at what differentiates a Layer 4 VPN from a Layer 3 VPN, and how a Layer 4 VPN meets the new requirements of mobile use cases more securely and more efficiently.

Design requirements for mobile VPN: Technological solutions

Fully mobile work imposes new requirements on secure VPN technology and connection. When an organization chooses a VPN for its mobile staff, there are different aspects that are important to consider:

- Seamless roaming: possibility of moving around without losing connection.
- Packet loss, delay & jitter: working on poor networks without losing connection.
- Low bandwidth: managing low network capacity.
- Battery capacity: avoiding rapid battery drain.



The OSI model is built in seven different layers, each of which indicates what type of technology is used for communication between services that are working in different layers.

As a rule, a traditional VPN sits on Layer 3, the network layer, and primarily applies the IPsec standard. With this kind of application, the VPN tunnel is established based on the IP addresses of the client and the server. In use cases where the IP addresses are stable and do not change during a session, this is an efficient choice.

Many of the challenges in mobile use cases, however, are easily solved if the VPN is designed to communicate on Layer 4. Such an application, which as a rule applies the TLS standard, establishes a session ID that the data transfer is linked to, instead of two IP addresses. The user is thus independent of whatever IP carrier—WiFi, 3G, 4G or 5G—is concerned. In mobile use cases, this yields significant advantages. In the following section, we will examine how Layer 4 VPN meets the new requirements of mobile use cases.

Possibility of moving around without losing connection

One of the key factors for successfully deploying field mobility is a security solution that offers a seamless user experience as the user moves around. Automatic roaming is essential as the device switches networks, moves in and out of coverage areas, and hibernates.

With a traditional Layer 3 VPN, the user needs to restart the session every time the client loses the connection to the server. As we have seen, this is because Layer 3-based data transfer is linked to the IP addresses allocated to the client and the server. When the client switches networks and thus temporarily loses the connection, which happens more or less frequently in a mobile use case, it often needs to be assigned a new IP address and a new connection to the server must therefore be established. For the user, this means having to be authenticated again. For example, if the user has a VoIP call running they will need to restart the call if the connection is lost.

A Layer 4 VPN is network-independent as it sits above the the network layer. The session stays open regardless of whether or not the client switches between networks, maintaining a continuous connection for both the user and the application. Since there are no specific requirements for network infrastructure equipment, a Layer 4 VPN is thus more reliable and robust.

Working on poor networks without losing connection

For the user to be able to work undisturbed even on poor networks, the VPN solution needs to overcome this challenge. Packet loss, delay and jitter are common occurrences in mobile networks, which lead to several complications for VPN solutions that operate on Layer 3. On the one hand, these phenomena could mean a new connection needs to be established, which as we saw in the previous section is a challenge for Layer 3 VPN since as a rule the user must be authenticated again, thereby resulting in a poor user experience. On the other, the fact that the Layer 4 standard operates higher up in the protocol stack of the OSI model yields the possibility of using intelligent flow control to smooth out the flow of data.

Managing low network capacity

In situations where the user only has access to limited bandwidth, or where the cost of data transfer is high, compressing the data to be transferred as much as possible may be important. This allows the user to make the best use of a limited network capacity. Furthermore, less data usage could mean a lower cost to the user depending on the operator's price models.

In basic use cases, this is not a serious problem, but in use cases where a lot of small packets are sent very frequently—real-time streams for VoIP calls, for example—there may be a noticeable difference for the user.

With the TLS protocol on Layer 4, the protocol overhead can be compressed more effectively than is possible with Layer 3 protocols, which lets the traffic make more efficient use of available capacity.

Avoiding rapid battery drain

One common challenge of Layer 4 VPN is that battery drain risks being relatively high if the mechanisms for minimising this are not applied by reducing signalling and radio transmitter use. The reason is that the protocol that operates on Layer 4 needs to send data relatively often to maintain a continuous connection, thereby providing the advantages we reviewed above.

To counteract this challenge of VPN on Layer 4, it is important when choosing a VPN to pay attention to which mechanisms the provider applies in order to optimise battery consumption.

Conclusion

Although Layer 3 and Layer 4 VPNs can be used in a similar manner, they are fundamentally different; they are designed for different use. Which solution is best for you depends on the situation and how the VPN will be used. The following guidelines should be considered when choosing a VPN solution that fits your organization:

- For cellular networks and situations when roaming can occur, a Layer 4 VPN is better suited.
- For static deployment between sites with large amounts of data being sent between nodes, a Layer 3 VPN is better suited.
- There is a risk that a Layer 3 VPN will not work over unknown and poorly-defined networks, since it must be supported by all nodes in the network. A Layer 4 VPN is a more reliable choice in such situations.

In addition to securing traffic between client and server, reviewing the security of the entire solution is appropriate. A mobile device such as a smartphone or tablet is more vulnerable since it runs a greater risk of being lost, stolen or attacked via vectors like Bluetooth, near field communication (NFC) and WiFi. How the entire platform is secured, and the extent to which sensitive data is stored locally on the device, should be considered. Read more in our article: Tips on working outside the usual office environment

The most important thing is to find a VPN solution that fits your organization, and the final choice depends on whether or not your workforce needs to be mobile. We recommend carefully going over all the points to determine which type of VPN you need to meet your specific needs, and the security requirements for working as efficiently and securely as possible.

Sectra AB • communications@sectra.com • communications.sectra.com

SECTRA
Knowledge and passion