

Top SD-WAN features



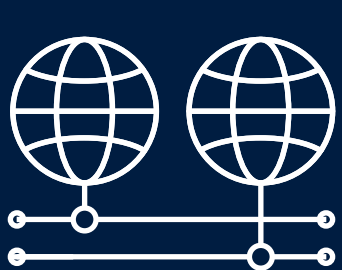
At a glance

Policy Based Routing



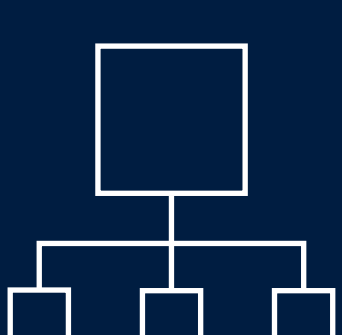
Control over which applications are allowed or blocked in company networks is crucial. This can be easily managed in the modern SD-WAN network: Policybased routing can be used to redirect or block applications, for example. For trustworthy applications, it is also advisable to prioritize the individual locations using a Local Internet Breakout. This reduces the load on the connection to the control center and improves the overall performance of the network.

Load Balancing



Active / Active mode, in which several Internet accesses at one location are used in parallel and distributed by load balancing, increases the available total bandwidth and enables dynamic load distribution. This mode supports the flexible and simultaneous use of all wired connections - be it Ethernet, fibre optic, DSL / cable via external modem or even mobile telephony.

Advanced Routing & Forwarding



ARF, or Advanced Routing and Forwarding, is a technology that makes it possible to set up separate communication channels for different user groups (such as accounting, development and management) via a central gateway. Each communication channel or IP context is isolated so that different participants can be given access to certain IP contexts as required, while other areas remain blocked.

High Scalability VPN (HSVPN)



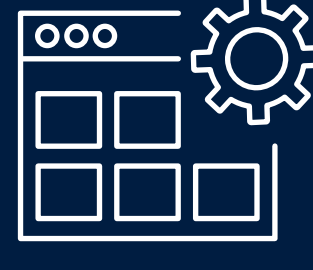
HSVPN significantly improves the scalability and efficiency of an SD-WAN architecture, especially in times of growing digitalization, increasing application diversity and rising data volumes. Instead of using a separate VPN tunnel for each application, HSVPN enables any number of networks to be bundled into a single VPN tunnel (secure tunnelling), which is transported to the remote site. The individual networks remain secure and strictly separated from each other. The advantage is a reduction in the number of VPN tunnels required and faster recovery times in the event of a failover.

Control & data plane



A key security feature of modern SD-WAN infrastructures is the strict separation between management (control plane) and data connections (data plane). While the data connections, such as VPN tunnels, are established directly between the VPN gateways, each network component communicates with an orchestrator via a separate management connection. This means that the user data remains invisible to the management system and the management and monitoring of the network components takes place independently of the data connections. This process is carried out fully automatically and without prior manual configuration of the devices (zero-touch provisioning) by establishing a secure connection from the device to the management system. By moving the control plane to a central cloud, the advantage is an always accessible, location-independent, centralized and web-based administration interface for all devices and applications at all locations.

Application Monitoring



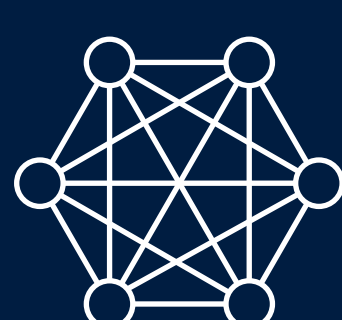
Nowadays, it is crucial to know which applications are being used in the network in order to be able to operate effective application management. A modern SD-WAN continuously monitors which users are using which applications and to what extent (top users / top applications). Historical logging and graphical analyzes provide a comprehensive overview that serves as the basis for well-founded network decisions.

Dynamic Path Selection



With Dynamic Path Selection, business-critical applications in an SD-WAN are always routed via the best available line. This feature continuously monitors all WAN connections with regard to load, packet loss, latency and jitter (Path Quality Monitoring), and dynamically selects the optimum line for certain applications based on the current connection quality. The Dynamic Path Selection algorithm decides on the line with the best performance. If several lines fulfill the defined guidelines, load balancing takes place in a round-robin process. As a result, users in extensive SD-WAN infrastructures with multiple WAN connections in active/active mode benefit from maximum performance and reliability.

Advanced Mesh VPN



In classic, star-shaped VPN site networks, where all branches are only connected via the head office and not directly to each other, the internet line at the head office often becomes a bottleneck for all communication. With Advanced Mesh VPN, the branch offices can communicate directly with each other, which reduces traffic at the head office and increases performance. The VPN tunnels are set up dynamically when data is transferred between the branches and are also dynamically dismantled again when communication is no longer taking place.

Firewall-Features



The digitalized present and sophisticated cyber attacks require new standards in network security. Application control, blocking, attack detection and prevention are essential for secure IT networks. Integrated into the powerful firewall operating system LCOS FX, these and other UTM security features "engineered in Germany" offer a considerable security advantage. The feature set of LANCOM R&S®Unified Firewalls and LANCOM vFi-rewalls is regularly expanded to protect professional networks against new types of risks.

