LANCOM Whitepaper

Cloud Management & Software-defined Networking

Conventional, static network architectures are no longer able to keep up with the ever-growing demands of modern enterprise infrastructures. Not only has the number of devices and network applications literally exploded, the distribution of sites has significantly broadened. What is more, IT administrators are confronted with increasing demands from users with regard to security and speed. The necessary manual configuration of individual network components generates massive workloads and resource bottlenecks. The solution to this dilemma is to outsource this complexity to an intelligent cloud-based management system that is based on software-defined networking. To exemplify the potential of this solution, this whitepaper shows how the administration of enterprise networks is dramatically simplified.

Limitations of current network architectures

A typical enterprise network needs to meet a variety of requirements: On the one hand, servers provide users with the data they need for their daily work. On the other hand, there are internal and external communications, both wired and wireless via Wi-Fi—and all of this at different locations with different applications and demands. In addition, a Wi-Fi hotspot is offered for guests and employees, securely separated from the internal productive network. Moreover, security against downtimes and attacks must be assured at all times.

In order to meet all these requirements, the configuration of all of the network components must be perfectly synchronized—routers, switches, access points and firewalls with agreed communication protocols, VLANs, QoS settings, firewall rules, authentication methods, and much more. Even for experienced, certified network administrators, the conventional configuration of individual devices can become an extremely time-consuming task: The workload and the number of errors increase exponentially with the number of devices, which can result in laborious troubleshooting for configuration errors.

On top of that, certain applications demand higher bandwidth and more optimized QoS on the spot. Manually meeting these requirements is not efficiently feasible. An automatic, application-centric system is needed as remedy.

Holistic network orchestration

Today's and the future requirements mean that networks will continue to be complex. In order for this complexity to remain manageable, we have to reconsider the ways that configuration and administration have been handled until now. Software-defined networking does away with the former manual configuration of individual devices and replaces it with the automated orchestration of networks. The administrator uses an easy-to-operate, centralized interface to specify the framework conditions for the overall network design. A central management system handles the configuration and rollout of respective changes—fully automatic and custom-designed for all of the network components (routers, gateways, switches, and access points). This ensures that the capabilities of the network components are utilized to the full, particularly in the area of virtualization. Another aspect is the strict separation of management connections on the control plane from data connections on the data plane: While the data connections (e.g. VPN tunnels) are set up between the VPN gateways, the individual network components are connected directly to the cloud-based administration system via independent management connections. What this means is: User data remain invisible to the management system while the management and monitoring of network components works (almost completely) independently of the data connections and their status. What is more, the whole system functions completely automatically by means of a secure connection from the device to the management system and without any prior configuration of the devices (zero-touch / auto-configuration).

Cloud-based management

Moving the control plane, i.e. the network management, to a central cloud offers the advantage of permanent, cross-site, out-of-band management along with a central, web-based administration interface for all devices, all sites, and all applications. It should be noted that there is a variety of concepts for hosting a cloud-based solution. While the location of the system and the access to the servers are handled differently, they all have in common that the content is accessible only to the administrator. The variants are as follows:

- Public Cloud

  This cloud-based management system is hosted in a public domain. It goes without saying that the Public Cloud ensures that customers and system integrators can only see and manage "their" own part of the network. The great advantage of this solution is: There are no costs or effort of commissioning. Installing and setting up the network can begin immediately after purchasing the necessary network products and cloud licenses. Important: When selecting a cloud hosting service provider, you should not only pay particular attention to the trustworthiness of the service provider, but also ensure the data center is located in a country with good data security standards. With the Public Cloud hosted in the EU, maximum data security and legally compliant handling are guaranteed.

- Private Cloud

  This cloud-based management system is operated at the data center of a Managed Service Provider (MSP). The MSP then uses the system to manage the network infrastructure of its customers. The great advantage of this solution: Significantly improved scaling as one management system can be used for all of it's customers. It also provides a corresponding level of privacy since the configuration data for the network remain in the data center of the MSP, who is known to the customer. The responsibility for the system lies clearly with the MSP.

- Self-hosted Cloud

  The cloud-based management system is installed and operated directly at the data center belonging to the end user. This variant offers the highest possible level of privacy as the configuration data does not leave the customer's network. At the same time it means the most work, since a management system has to be installed and operated for just one customer.

Software-defined networking

Orchestration of the complete network includes the WAN, LAN, WLAN and SECURITY, and all of the associated network functions (Figure 1). This is why the terms SD-WAN, SD-LAN, SD-WLAN and SD-SECURITY have become established. The basic principle of software-defined networking (SDN) is the shift away from device-centric to a network-centric, even application-centric approach. Here, only networks and traffic connections are defined. The concrete implementation is handled by the central, automated instance and the devices themselves.

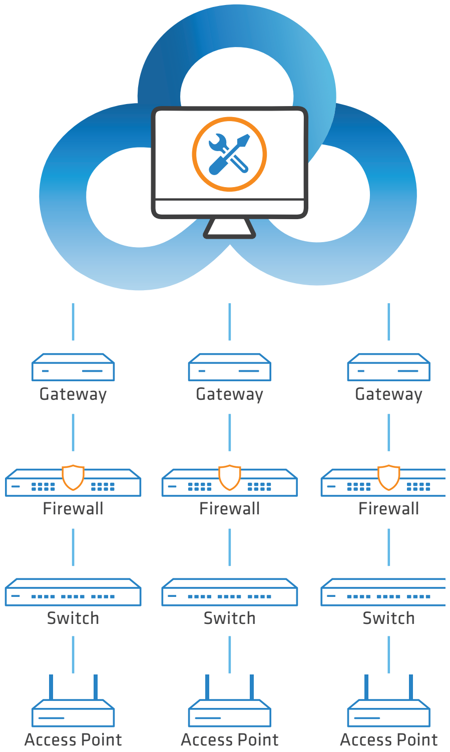

Fig. 1 Software-defined networking

SD-WAN

SD-WAN automatically creates secure IPSec VPN connections between sites, including network virtualization across the WAN. A few mouse clicks is all it takes to enable the VPN function and select the required VLANs for each site. The laborious configuration of individual tunnel endpoints is no longer required at all.

SD-LAN

SD-LAN orchestrates the port profiles for each switch and automatically assigns the necessary network configuration, e.g. the required VLANs. Each VLAN represents a segment within the overall network. At the click of a mouse, switch configurations that are fully customized for the access points and routers at each site are rolled-out or updated simultaneously.

SD-WLAN

SD-WLAN facilitates the automatic configuration of multiple Wi-Fi networks (multi-SSID) including, for example, the separation of hotspot networks. These different Wi-Fi networks can be regarded as segmentation within the whole network. All that needs to be specified here is the SSID authentication method and, if required, the bandwidth restrictions for each Wi-Fi network. The Wi-Fi profiles created in this way are rolled out or updated on any number of access points and Wi-Fi routers at the different sites – again, simply by mouse click.

SD-SECURITY

SD-SECURITY ensures highly automated security functions of cloud-managed next-generation UTM firewalls. With centralized administration of network security, compliance and bandwidth usage policies, applications can be blocked or direct access can be allowed.

Summary

Software-defined networking does away with the previously manual configuration of devices and replaces it with automated network orchestration. It establishes a central, cloud-based management system that uses SDN technology as the basis for a holistic, "hyper-integrated" management. In other words: It takes care of all devices, whether routers, switches, access points or firewalls. This greatly reduces the operating expenses (OPEX): Eliminating the laborious configuration of individual devices, new sites are integrated faster and with greater security, network errors can be identified quickly and fixed proactively – without having to dispatch expensive field engineers. In addition, the individual network segments can be modified globally, the changes are automatically rolled out to all of the relevant devices, and monitoring is centralized and comprehensive. Administrative tasks that previously took hours or days to complete are now taken care of within minutes or a few clicks. The result: Complex networking scenarios are easy to master, and networks and application services are brought to a new level of performance.