LANCOM Systems and macmon secure cooperate in the field of Network Access Control (NAC)

LANCOM Systems GmbH is a European provider of modern network infrastructure components (WAN, LAN, WLAN, firewalls), virtual network components, and a cloud-based system for the central administration of the entire network portfolio. The LANCOM product portfolio is suitable for addressing a wide variety of networking scenarios. Customers are mainly commercial enterprises of different sizes as well as public administrations, universities, and schools.

Rounding off the offerings for the prevention of unauthorized access to the network, LANCOM cooperates with the NAC provider macmon secure GmbH, who has been offering vendor-independent solutions for protecting against unauthorized access to heterogeneous networks since 2003.

A powerful duo

The advantage of this cooperation is the compatibility offered by the solutions from these two providers. The full range of macmon NAC functions work seamlessly with LANCOM network components and their integrated security functions. This guarantees a high level of security for customers. The cooperation between the two German manufacturers means that Network Access Control (NAC) will become an integral part of LANCOM networking solutions.

How does macmon NAC work?

First of all macmon NAC scans all of the switches and connected end devices to provide a complete overview of the devices on the network and where they are located. This ensures that only authorized devices known to the network management are able to use the (W)LAN. If an unknown device logs in to the network, an alert is issued immediately and countermeasures can be initiated automatically. For control over access, macmon uses a reactive approach based on SNMP or a proactive approach that uses IEEE 802.1X, both of which can be used in mixed operation.

Please note that NAC-SNMP must not be operated together with the LANCOM Management Cloud. In this case, the two management systems would interfere with each other and the last configuration written in each case would be used. Therefore, only use this method together with standalone switches.

We recommend using NAC via RADIUS because it can be operated both with standalone switches and with the LANCOM Management Cloud. In addition, it uses much higher-quality authentication methods in the process and offers some advantages over NAC-SNMP.

LANCOM
SYSTEMS

Differences between NAC-SNMP and NAC over RADIUS

With NAC-SNMP, the MAC addresses are learned at the switch port, and exactly one VLAN can be assigned to the respective switch port. If another unmanaged desktop switch is connected to this port, all connected devices have the same VLAN; if there are conflicting authorizations, a good decision for a target VLAN cannot be implemented.

In addition to authentication via EAP method using the user name with password or a certificate, with NAC via Radius it is also possible to make the MAC address as such a criterion (MAC fallback / MAC authentication bypass). In addition, VLAN assignment can occur not only at port level but also at session level, so that more than one end device can be connected with individual VLAN switching per port.

To ensure that the radius switching on the port is not disturbed by the configuration written by the LANCOM Management Cloud, you should generally allow all VLANs on the ports in the LANCOM Management Cloud. The radius then controls which VLAN is used in each case.
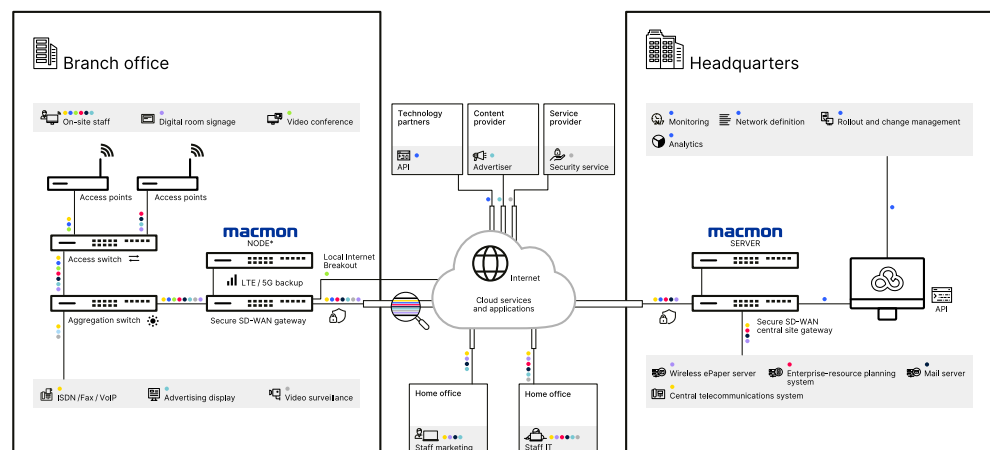
Furthermore, standardized and automatically applied security rules allow or prevent access to the corporate network infrastructure. This is vital in times of increasing numbers not only of user devices but in particular the fast proliferation of cyber-physical devices such as IoT (Internet of Things) and OT (operational technology) devices. All devices on the network are constantly checked for their compliance with policy. If a device deviates from a previously defined policy, e.g. the virus scanner is out of date or the firmware of a client is outdated, the client can be placed in quarantine. The client is only granted access again when the updates are installed and the device status complies with the defined policies.

This double protection mechanism ensures that only trusted end devices operate on the network and that they meet all the requirements of the security policy. This prevents unauthorized devices from entering the network via the WLAN gateway or an available network socket. It also closes the human security gap in the form of employees who, through carelessness or even on purpose, do not observe the security guidelines for devices on the network.

Modern client management and BYOD through NAC

The combination of the LANCOM infrastructure with the macmon NAC solution also offers outstanding applications wherever users are offered BYOD (bring your own

Figure 1:
NAC with macmon

Receives its configuration from the macmon server; the NAC service is maintained if the VPN connection to the central office is terminated.

device)—for example where students and teachers in schools have separate networks. Users can log in to the organization's (e.g. school) Wi-Fi with their smartphones or tablets, and macmon Network Access Control then creates an overview of the devices on the network. These third-party devices are given access to a network that is isolated from the organization's internal network segments, e.g. for the administration and authorized devices such as PCs, printers or laptops. Every unauthorized access attempt is immediately identified, efficiently monitored and, if necessary, blocked. Devices belonging to people from outside the organization can be given access to a separate guest area. Access to the mission-critical network segments is therefore reserved for employee devices. Private devices of employees or students (BYOD) can be granted access rights to certain internal areas if they comply with certain policies.

Network sockets as gateways to networks

A further Achilles' heel for any network are any freely accessible network sockets in company or clinic buildings. It is important for all network sockets to be patched with the ports of LANCOM access switches. The LANCOM Management Cloud globally roll out all of the desired networks on specified ports of all switches at all managed locations. After this basic VLAN configuration, the macmon NAC solution can be used to make custom adjustments for individual users, devices or projects: If a third-party device is detected on the network, the NAC system issues a command to the relevant switch to reconfigure the network port. If an unknown device is connected and detected, the network port is switched off and the device immediately loses its network connection.

Versatile design of workplaces and access authorizations

An option with NAC is not to block the network ports as described above, but to redirect them instead: An unknown client logging on to the network in this case is not completely separated from the network. Instead, it is redirected to the guest-area login page, where they can register to gain access to the Internet. Along with the security aspect, this function also offers a convenient way of controlling VLANs for employee devices. In this case, macmon knows the VLAN belonging to the end device (and the port) and automatically provides all of the resources that employees need, wherever the end device is connected. This is outstanding added value, especially for companies that no longer have fixed arrangements in their offices and workplaces.

Feel free to contact us and take your network security to the next level! Please contact the LANCOM Inside Sales office in Germany.

Telephone: +49 (0)2405 49936 122

LANCOM
SYSTEMS