10 THINGS YOU NEED TO KNOW

about Cloud-Managed Network Access Control (NAC)

1



NAC is built on an 802.1X Framework

The 802.1X components (supplicants, authentication gateway, authentication server) work together to make sure only properly validated users and devices can access the appropriate network resources.

2



The Security Concept of AAA is Central to NAC

Authentication, Authorization and Accounting (AAA) is a key network security concept and is the original core functionality of Network Access Control. Modern NAC solutions extend beyond AAA with additional, value-added functionality.

3



Today's NACs Provide Certificate Onboarding

Modern NACs include onboarding solutions that can configure clients with 802.1X certificates, and often provide automated self-service workflows for this purpose.

4



Access Control is Vital

Role-based access control (RBAC) is used to restrict network access to authorized users, based on their corporate role. The system uses RADIUS attributes to ensure users get the appropriate VLAN, access to network resources, bandwidth allocation and much more.

5



Posture Assessment Ensures Endpoint Integrity

Posture assessment ensures that endpoints stay secure over time by validating up-to-date versions of device OS, antivirus, antimalware signatures, and application patches. Devices that don't comply can be quarantined until they are updated.



Guest Management is a Key Component

NAC security requires a means to provide wired or wireless guest access while protecting the corporate network. At a minimum, guest access should require a separate guest SSID, a unique guest VLAN, and a guest firewall policy.

G



... as is BYOD Management

Employees expect to be able to user their personal devices on the company network.

NAC must support BYOD policies that dictate which corporate resources can or cannot be accessed when employees connect to the company network with their personal devices.



Device Identity is Crucial

Device fingerprinting reliably identifies the types of devices requesting access to the corporate network and provides network administrators visibility into the device population. NACs can also block network access altogether for certain types of devices.

8



IoT Security is a Requirement for Today's NACs

A population explosion of IoT devices onto enterprise networks has already begun.

A good NAC solution with device fingerprinting capabilities is necessary to identify and classify IoT devices so that proper access policies can be enforced.

9



Cloud-Managed NAC is the Future

A cloud-managed NAC centralizes monitoring and configuration of remote sites, while localized tasks like device authentication and access control enforcement are executed onsite. Centralized NAC management streamlines NAC operations and increases operational efficiency.

10

