NETWORK ACCESS CONTROL (NAC)

YOUR NETWORK, YOUR RULES. NETWORK ACCESS UNDER CONTROL.

Abuse of unsecured networks remains one of the most common attack vectors in organisations across the EU. If an organisation does not have control over who and what connects to its network, the risk of unauthorised devices or attackers gaining access increases significantly. A lack of proper segmentation allowing unrestricted movement of threats within the network typically leads to the rapid spread of malware or ransomware. Outdated devices or those that have not been updated for some time often go unnoticed and are the cause of critical vulnerabilities. Last but not least, organisations risk non-compliance with new legislation (ZoKB / NIS2).

ABOUT THE NAC SERVICE

Our NAC service is built on Aruba Networks' advanced ClearPass platform. It is a modern solution for secure management of access to corporate networks that provides you with full control over network access for your employees, visitors, and contractors. The service is defined in several standardised operational scenarios that differ primarily in the configuration of the **ClearPass Policy Manager** (CPPM)* as the core component of the entire platform, based on the number of licensed customer devices selected. The service can be operated either primarily for network access control purposes (802.1X, MAC, TACACS+) or with an advanced functionality that also includes health verification of all devices (known as posture checks).

HOW DOES THE NAC SERVICE WORK?

1. DEVICE AND USER IDENTIFICATION AND AUTHENTICATION:

- Anyone attempting to connect to the network (wired, Wi-Fi, VPN) is automatically identified: device, user, operating system type, location, and security posture.

2. POLICY-BASED EVALUATION AND DECISION:

- Based on predefined policies, the system determines whether a device is granted access, what type of access it receives, or whether access should be denied or restricted.

3. DYNAMIC ACCESS CONTROL AND RESPONSE:

- The system grants or modifies access in real time, segments the network, isolates threats, and can notify the security team or respond automatically (e.g. by disconnecting a device).

PARAMETERS OF THE NAC SERVICE

Operational Scenarios / Environment		„S“	„M“	„L“	„XL“
CPPM*	Publisher	✓	✓	✓	project-based
	Publisher (StandBy)	✗	✓	✓	
	Subscriber	✗	✗	✓	
Recommended number of devices (licenses)		< 1000	< 5000	< 15000	> 15000

* The NAC service architecture distinguishes the roles of **Publisher, Standby Publisher,** and **Subscriber.** These represent individual nodes in a multi-instance CPPM environment, typically deployed in an HA cluster or distributed architecture. CPPM can be operated in the CRA cloud environment, the customer's own infrastructure, or in public cloud environments such as Microsoft Azure or Amazon AWS.

SECURITYHUB

The NAC service includes a portal (the CRA Security Hub) that provides customers with an online overview of the status of their infrastructure in the form of clear charts and tables. It supports management-level views and role-based access rights. The portal also includes integration with the native Aruba ClearPass Insight platform.

WHO IS THE NAC SERVICE FOR?

FOR WHOM	KEY BENEFITS	BENEFIT FOR CUSTOMER
Corporations and Large Enterprises	• Centralised policies across multiple locations. • Detection of unauthorised devices. • Integration with EDR, SIEM, and MDM.	• A scalable and auditable NAC solution with the possibility of integration into a comprehensive security stack.
Industry and Manufacturing	• Separation of IT and OT networks. • Detection and classification of IoT/OT devices. • Protection of SCADA/ICS systems.	• Operational continuity and robust cybersecurity protection is ensured in industrial environments.
Finance and Banking	• Advanced risk-based access control. • Integration with compliance systems (DLP, SIEM). • Compliance with DORA, NIS2, GDPR.	• Risk minimisation, high-level protection of sensitive data, and auditability.
Public Sector	• Strong authentication and role-based access. • Supporting legislation (ZKB, NIS2, GDPR). • Transparent management with audit trails.	• Higher level of trustworthiness and control over access in a sensitive infrastructure.
Healthcare	• Secure access for staff, patients, and guests. • Support for IoMT (medical devices). • Integration with MDM and EMR (Electronic Medical Records) • Compliance with legislation (GDPR, ZKB)	• Protection of sensitive data and a secure infrastructure for healthcare facilities.
Education and Universities	• Wi-Fi onboarding for students and guests. • BYOD portals. • Role-based access by user type. • Identity audit and management.	• Secure connection in an open campus environment without compromised flexibility.

BENEFITS OF THE NAC SERVICE

- **Device visibility across the customer's network** – elimination of blind spots and rapid response to unknown or unauthorised devices.
- **Identity- and context-based access control** – only authorised users gain access – and only to the resources they are permitted to use.
- **Compliance with security policies and regulations ensured** – simplified process of documenting compliance during internal and external audits.
- **Network segmentation** – limiting damage in case of compromise as the attacker cannot get farther than to what they really need.
- **Automated security response** – rapid incident response free of human error or delays. Integration with SIEM, EDR, or other customer technologies is not part of the Service.
- **Device onboarding and BYOD management** – high user comfort without compromising on security.
- **Easy integration into existing architecture** – no need to replace infrastructure; NAC adapts to the customer environment.

Do you know who is in your network right now? With NAC, you will know for sure. Investing in the NAC service is a key step toward verifying the identity of users and devices connecting to your network. Protect your network smartly and with full visibility. For more information or a tailored consultation, visit our website or contact our team of experts (obchod@cra.cz).