# NETWORK ACCESS CONTROL (NAC)

## VAŠE SÍŤ. VAŠE PRAVIDLA. SÍŤOVÝ PŘÍSTUP POD KONTROLOU.

**Zneužití nezabezpečených síťových přístupů je stále jedním z nejčastějších vektorů útoku v organizacích v EU. Pokud nemá organizace kontrolu nad tím, kdo a co se připojuje do její sítě, výrazně zvyšuje riziko vniknutí neautorizovaných zařízení nebo útočníků. Chybějící segmentace umožňující volný pohyb hrozeb po síti obvykle vede k rychlému šíření malware nebo ransomware. Zastaralá nebo neaktualizovaná zařízení bez povšimnutí způsobují kritické zranitelnosti. V neposlední řadě organizace riskuje nesoulad s novou legislativou (ZoKB/NIS2).**

## O SLUŽBĚ NAC

Naše služba NAC je postavena na vyspělé platformě ClearPass od společnosti Aruba Networks. Jedná se o moderní řešení pro bezpečnou správu přístupu do firemní sítě. Díky tomu získáte plnou kontrolu nad přístupem do sítě pro vaše zaměstnance, návštěvníky nebo dodavatele. Službu definujeme v několika typizovaných provozních scénářích, které se liší především v setupu **ClearPass policy managera** (CPPM)*, jakožto hlavní komponenty celé platformy, a to při zvoleném počtu licencovaných zařízení zákazníka. Službu lze provozovat s primárním účelem pro řízení přístupu k síti (8021X, MAC, TACACS+), anebo s pokročilou funkcionalitou zajišťující i zdravotní kontrolu všech zařízení (tzv. Posture check).

## JAK SLUŽBA NAC FUNGUJE?

### 1. IDENTIFIKACE A OVĚŘENÍ ZAŘÍZENÍ I UŽIVATELŮ:

- Každý, kdo se pokusí připojit do sítě (kabelové, Wi-Fi, VPN), je automaticky rozpoznán: zařízení, uživatel, typ OS, poloha a stav zabezpečení.

### 2. VYHODNOCENÍ A ROZHODNUTÍ PODLE POLITIK:

- Na základě nastavených pravidel systém rozhodne, zda má dané zařízení přístup, jaký typ přístupu, nebo jestli má být přístup odepřen nebo omezen.

### 3. DYNAMICKÉ ŘÍZENÍ PŘÍSTUPU A REAKCE:

- Systém v reálném čase uděluje nebo mění přístup, segmentuje síť, izoluje hrozby a může informovat bezpečnostní tým či automaticky reagovat (např. odpojením zařízení).


## PARAMETRY SLUŽBY NAC

| Provozní scénáře / prostředí | | „S“ | „M“ | „L“ | „XL“ |
|---|---|---|---|---|---|
| CPPM* | Publisher | ✓ | ✓ | ✓ | projektově |
| | Publisher (StandBy) | ✗ | ✓ | ✓ | |
| | Subscriber | ✗ | ✗ | ✓ | |
| Doporučení pro počet zařízení (licencí) | | < 1000 | < 5000 | < 15000 | > 15000 |

*Architektura služby NAC rozlišuje role „Publisher“, „StandBy Publisher“ a „Subscriber“. Jedná se o jednotlivé uzly (nody) v prostředí s více instancemi CPPM, typicky v HA clusteru nebo distribuovaném prostředí. CPPM může být provozován v cloudovém prostředí CRA, organizace nebo ve veřejném prostředí MS Azure či Amazon AWS.

## SECURITYHUB

Součástí služby NAC je Portál (CRA Security Hub), který zákazníkům přináší online přehled o stavu jeho infrastruktury formou přehledných grafů a tabulek. Umožňuje manažerské pohledy a definici oprávnění dle rolí uživatelů. Součástí portálu je také napojení na nativní portál platformy Aruba ClearPass Insight.

## PRO KOHO JE SLUŽBA NAC URČENA?

| PRO KOHO? | KLÍČOVÉ VÝHODY | PŘÍNOS PRO ZÁKAZNÍKA |
|---|---|---|
| Korporace a velké společnosti | • Centralizované politiky pro více lokalit.<br>• Detekce neautorizovaných zařízení.<br>• Integrace s EDR, SIEM, MDM. | • Škálovatelné a auditovatelné NAC řešení s možností integrace do komplexního security stacku. |
| Průmysl a výroba | • Oddělení IT a OT sítí.<br>• Detekce a klasifikace IoT/OT zařízení.<br>• Ochrana SCADA/ICS systémů. | • Zajištění provozní kontinuity a kybernetická ochrana v průmyslových provozech. |
| Finance a bankovnictví | • Pokročilé řízení přístupu dle rizika.<br>• Integrace s compliance systémy (DLP, SIEM).<br>• Soulad s DORA, NIS2, GDPR. | • Minimalizace rizik, vysoká úroveň ochrany citlivých dat, auditovatelnost. |
| Veřejná správa | • Silná autentizace a role-based access.<br>• Podpora legislativy (ZKB, NIS2, GDPR).<br>• Transparentní správa s auditními stopami. | • Vyšší úroveň důvěry a kontrolovatelnosti všech přístupů v citlivé infrastruktuře. |
| Zdravotnictví | • Bezpečný přístup pro personál, pacienty i hosty.<br>• Podpora IoMT (medicínská zařízení).<br>• Integrace s MDM a EMR (elektronická zdravotnická dokumentace).<br>• Soulad s legislativou (GDPR, ZKB). | • Ochrana citlivých dat a bezpečná infrastruktura pro zdravotnická zařízení. |
| Školství a univerzity | • Wi-Fi onboarding pro studenty a hosty.<br>• Portály pro BYOD.<br>• Role-based access podle typu uživatele.<br>• Audit a správa identit. | • Zabezpečené připojení v otevřeném kampusovém prostředí bez ztráty flexibility. |

## VÝHODY SLUŽBY NAC

- **Viditelnost zařízení v síti zákazníka** – eliminace „slepých míst“ v síti a možnost rychle reagovat na neznámá nebo neautorizovaná zařízení.
- **Řízení přístupu podle identity a kontextu** – přístup dostane jen ten, kdo má právo – a jen k tomu, k čemu má mít přístup.
- **Zajištění souladu s bezpečnostními politikami a regulacemi** – zjednodušení prokazování souladu při interních i externích auditech.
- **Segmentace sítě** – omezení škod při kompromitaci, protože útočník se nedostane dál než k tomu, co skutečně potřebuje.
- **Automatizace bezpečnostních reakcí** – rychlá reakce na incident bez lidské chyby nebo zpoždění. Integrace na SIEM, EDR nebo další technologie zákazníka není součástí Služby.
- **Onboarding zařízení a správa BYOD** – uživatelský komfort bez kompromisu v bezpečnosti.
- **Snadná integrace do stávající architektury** – není nutné měnit infrastrukturu, NAC lze přizpůsobit prostředí zákazníka.

Víte, kdo je právě teď ve vaší síti? S NAC budete mít jistotu. Investice do služby NAC je zásadním krokem k ověření identity uživatelů a zařízení připojujících se do vaší sítě. Chraňte svou síť chytře a s přehledem. Pro více informací a konzultaci na míru navštivte naše webové stránky nebo kontaktujte náš tým odborníků (obchod@cra.cz).