**Příloha č. 4 – Technická specifikace**

Systém musí splňovat následující minimální (nepodkročitelné) technické požadavky:

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Minimální požadavky** | **Splňuje ANO/NE** |
| Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení | Ano |  |
| Forma dodání: virtuální appliance pro VMware | Ano |  |
| Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení | 500 |  |
| Řešení musí poskytovat vysokou dostupnost tak, aby v případě výpadku primárního serveru převzal jeho roli sekundární server | Ano |  |
| Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru. | 30 |  |
| Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance. | Ano |  |
| Multiplatformní podpora minimálně 10ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě) | Ano |  |
| Požadované metody autentizace uživatelů a zařízení | PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace |  |
| Podpora RADIUS CoA | Ano – dle RFC3576 |  |
| Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD | Ano |  |
| Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období | Ano |  |
| Možnost TACACS+ autentizace správců síťových zařízení | Ano |  |
| Další požadované autentizační a autorizační zdroje a metody | LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta) |  |
| Možnost integrace s MDM (Mobile Device Management) platformami třetích stran | minimálně AirWatch, Citrix, MobileIron, JAMF |  |
| Podpora REST API pro většinu základních úkonů platformy | Ano |  |
| Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) | Ano |  |
| Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení | Ano |  |
| Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran | Ano |  |
| Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě | Ano |  |
| LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS a email ověřením | Ano |  |
| Systém musí obsahovat licenci nejméně pro 100 současně připojených unikátních hostovských zařízení | Ano |  |
| Hosté či interní uživatelé musí mít možnost přístupu do samoobslužného portálu pro správu svých vlastních registrací | Ano |  |