# Technická specifikace předmětu plnění - Komplexní řešení řízení přístupu k síti OU

Zadavatel požaduje dodání a implementaci komplexního řešení pro přístup do sítě pro zvýšení a zajištění síťové bezpečnosti.

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží (software)** | |
| Typ/jméno nabízeného software v rámci řešení a jeho verze |  |
| Výrobce |  |

Níže jsou uvedeny požadavky, který musí systém pro řízení přístupu do sítě splnit:

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **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 a pro KVM | ano |  |
| Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení | 6000 v redundantním clusteru |  |
| Řešení musí poskytovat vysokou dostupnost tak aby v případě výpadku primárního AAA serveru převzal jeho roli automaticky 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 |  |
| Podpora minimálně 20ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě): 3com, Alcatel, Aruba, Brocade, CheckPoint, Cisco, Colubris, Digium, Fortinet, HPE, Juniper, Lucent, Meraki, Mikrotik, Motorola, Nexans, PaloAlto, Ruckus, SonicWall, Zyxel | ano |  |
| Požadované metody autentizace uživatelů a zařízení | PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP), MAC autentizace, MPSK |  |
| Podpora autorizace pomocí externího Cloud zdroje identity: Azure Active Directory. | ano |  |
| ‍Podpora vícefaktorového ověřování | ano |  |
| Podpora RADIUS CoA - RFC3576 | ano |  |
| Podpora autorizace zařízení a uživatelů na základě kontextových informací, minimálně tyto parametry: 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, InTune |  |
| Podpora REST API pro většinu základních úkonů AAA platformy (minimálně pro: vytvoření, výpis, modifikace, smazání uživatele, zařízení, MAC) | ano |  |
| Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) | ano |  |
| Podpora komunikace s externí SMS bránou protokolem HTTP/HTTPS, SMTP, SMPP | 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”), min. DHCP volby klienta, HTTP uživatelský agent, výrobce dle MAC adresy, operační systém. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě. | ano |  |
| ‍Možnost provisioningu koncových zařízení s OS MS Windows, Android, MacOS/iOS, Linux (automatizovaná konfigurace síťového připojení, instalace SSL certifikátu) | ano |  |
| ‍Podpora jazykových mutací samoobslužného portálu, min. CS, EN, DE, FR, IT, ES, PL, RU, včetně návazných SMS zpráv, mailů, GUI | ano |  |
| ‍Systém musí umožňovat logické oddělení autentizace a registrace uživatelů dle SSID nebo jiných síťových parametrů bez nutnosti plné multitenantní architektury. | ano |  |
| **Guest (řízení přístupu hostů-Captive Portal LAN a WiFi)** | | |
| Podpora HTTP a HTTPS web autentizace (Captive portál). | ano |  |
| Podpora CAPPORT - RFC 8908 | ano |  |
| Podpora autentizace hostů pomocí účtů sociálních sítí: Google+, Facebook, Twitter, LinkedIn. | ano |  |
| Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autentizační kód. | ano |  |
| Možnost samoobslužné registrace hosta do sítě se SMS a email ověřením. | ano |  |
| Možnost přístupu pouze s akceptací podmínek užití. | ano |  |
| Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat. | ano |  |
| Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů: doba platnosti, objem přenesených dat, časové okno, počet souběžných přihlášení | ano |  |
| Perzistence autentizace/registrace s využitím MAC cache a zobrazení jen uvítacích stránek s osobním oslovením hosta při opakovaných návštěvách. Konfigurovatelné hodnoty trvání MAC cache pro různé hosty v rámci jedné služby (např. jedno SSID). | ano |  |
| Možnost vytváření účtů samoobslužnou registrací. | ano |  |
| Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace. | ano |  |
| Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů umožňuje minimálně:   * Úprava barev, fontů, pozadí a loga. * Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu. * Možnost vkládání animací, videí a dalšího dynamického obsahu.   Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store). | ano |  |
| **Podpora BYOD** | | |
| Bezpečná registrace soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém). | ano |  |
| Certifikační autorita pro vydávání certifikátů na soukromá zařízení musí být součástí AAA platformy. | ano |  |
| Systém musí podporovat zaregistrování soukromých zařízení s vygenerovaným certifikátem. | ano |  |
| Hosté či interní uživatelé musí mít možnost přístupu do samoobslužného portálu pro správu svých vlastních registrací. | ano |  |
| Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení. | ano |  |
| Možnost licenčního rozšíření o kontrolu stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku | ano |  |
| Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. | ano |  |
| Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem | ano |  |
| Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém. | ano |  |
| **Management** | | |
| HTTPS rozhraní s podporou konfiguračních průvodců a předkonfigurovaných šablon. | ano |  |
| Diagnostika problémů (systémová, údaje o chybách přihlašování, packet capture včetně filtrů) | ano |  |
| Appliance podporuje šifrování disku nebo souborů. | ano |  |
| Appliance podporuje CLI přístup a umožňuje v něm konfiguraci základních nastavení. | ano |  |
| **‍Technická podpora** | | |
| Servisní podpora po dobu 60 měsíců. Možnost otevírat servisní požadavky po dobu 60 měsíců od předání a odstranění všech vad a nedodělků v režimu 24x7, zahájení řešení během aktuálního pracovního dne nebo následujícího pracovního dne, pokud je svátek, víkend, den pracovního klidu | ano |  |
| Dostupnost softwarových aktualizací (nové verze programového vybavení) po dobu minimálně 60 měsíců od převzetí. | ano |  |
| ‍Dodání náhradních dílů výrobce: následující pracovní den (NBD) | ano |  |
| Možnost rozšíření celkové kapacity řešení (počet unikátních koncových zařízení) | ano |  |
| **Ostatní** |  |  |
| Účastník je výrobcem nabízeného řešení, příp. certifikovaným obchodním a servisním zástupcem výrobce nabízeného řešení | ano |  |