# Technická specifikace – Část 4 Aktivita 1 Realizace nástroje pro řízení přístupu na síti

Obsah

[1) Popis obecných požadavků na systém 3](#_Toc197342382)

[**Řešení přístupu zařízení a uživatelů do LAN a WLAN včetně segmentace** 3](#_Toc197342383)

[2 Specifikace minimálních požadavků technického řešení 5](#_Toc197342384)

# Popis obecných požadavků na systém

**Řešení přístupu zařízení a uživatelů do LAN a WLAN včetně segmentace**

Součástí navrženého řešení řízení přístupu zařízení a uživatelů (autentizace a autorizace) je konfigurace aktivních prvků, kontrolérů a autentizačního, autorizačního a účtovacího serveru (dále jen AAA server) minimálně v rozsahu v této kapitole uvedeném. AAA server je součástí návrhu celého řešení a bude nakonfigurován a zalicencován v redundantním zapojení (HA režim). Oba tyto servery budou nainstalovány do navrženého virtuálního v prostředí nemocnice.

Systém řízení přístupu zařízení a uživatelů do LAN a WLAN bude realizován primárně pomocí 802.1X, která je zajištěna třemi zásadními komponentami:

1. Konfigurovatelné **aktivní prvky s podporou 802.1X**, CoA (RFC 3576) a WebAuth.
2. **AAA server** (specializovaný server RADIUS), který podporuje **autentizaci EAP protokoly** (zejména EAP-TEAP, EAP-PEAP a EAP-TLS). Mimo to podporuje autentizaci MAB a pomocí WebAuth portálů. Podporuje také napojení na různé zdroje identit a systémy 2FA.
3. **Zařízení s 802.1X supplicantem podporující uvedené EAP protokoly**.

Zařízení, která nepodporují 802.1X budou autentizována pomocí náhradních metod ověření – MAB, WebAuth, PSK založené na atributech zařízení (skupina MAC, lokalita apod.)

Všechny veřejně přístupné porty síťových přepínačů budou nakonfigurované pro ověřování pomocí 802.1X, MAB a případně WebAuth (dle analýzy požadavků zadavatele). Zařízení bude ověřeno na AAA serveru a dle definované politiky mu budou přiděleny práva na portu switche. Ověřené zařízení dostane na všech portech stejná práva. V případě, že zařízení je možné připojit do bezdrátové i drátové sítě, pak stejná práva má nezávisle na použité konektivitě.

**Lokální počítačová síť – drátová (LAN)**

Switch ověří zařízení prostřednictvím **protokolu 802.1X** a pokud projde ověřením, přidělí mu příslušná práva dle definovaných politik. Pokud zařízení neumí 802.1X či dojde při ověřování k chybě, pokusí se zařízení ověřit podle MAC adresy (MAB – MAC Authentication Bypass). Pokud je MAB úspěšný, zařízení opět dostane práva dle definovaných politik. Pokud je MAB neúspěšný, budou nakonfigurovány politiky na základě analýzy požadavků zadavatele – např. WebAuth v zasedací místnosti, instalační VLAN na definovaných zásuvkách apod.

**Politiky budou definovány** minimálně pro tyto dva typy zařízení:

*Doménový počítač (typicky zařízení s OS WIN)*

* Počítač i přihlášený uživatel MUSÍ být v doméně (AD).
* Počítač v AD bude zařazen v příslušné skupině nebo OU (organizační jednotka).
* Počítač má z AD vygenerovaný certifikát, který použije k přihlášení (počítače odstraněné z domény nesmí být vpuštěny do sítě i v případě platnosti certifikátu).
* Počítač, před přihlášením uživatele do domény, dostane práva na přihlášení uživatele do domény.
* Po přihlášení uživatele, do domény, bude počítač reautentizován a dojde k současnému ověření počítače a uživatele (metoda EAP-TEAP nebo EAP-FAST podporující EAP-Chaining).
* Počítači bude přidělena VLAN kde se dostane do interní sítě a má přístup na servery.

*Tiskárny, scannery apod. (ostatní zařízení, které neumí protokol 802.1x)*

* Zařízení bude definováno na AAA serveru (administrátorem nebo pověřeným zaměstnancem s omezenými právy).
* Účet bude mít definovánu skupinu nebo přímo VLAN.
* Tyto zařízení budou mít zpravidla dedikovanou VLAN, případně speciální VLAN s omezením práv pomocí ACL (Access List).

Dále mohou být **definovány skupiny návštěvníků a soukromých zařízení, které mohou být ověřovány** např. pomocí WebAuth portálu, případně může být jejich přístup omezen např. vyhrazenými porty (při zachování autentizace pro doménové počítače i IoT zařízení), časem přístupu apod.

**Lokální počítačová síť – bezdrátová (WLAN)**

Bezdrátová síť využívá stejný způsob ověřování jako LAN pouze s tím rozdílem, že se uživatel nepřipojuje do ethernetového portu („datové zásuvky“), ale připojuje se prostřednictvím přístupových bodů a ověření probíhá prostřednictvím kontroléru. Bezpečnost je jednotná pro LAN tak WLAN tzn. způsob autentizace je pro zaměstnance, pacienty, síťové administrátory a notebooky totožný.

V bezdrátové síti budou nakonfigurovány tyto typy bezdrátových sítí (SSID):

* Interní SSID – zařízení používající 802.1X k autentizaci
* IoT SSID – zařízení, která nepodporují autentizaci 802.1X, ale využívají nebo jsou využívány prostředky v interní síti. Tyto zařízení využívají autentizaci pomocí PSK (PreShared Key), které je unikátní pro zařízení nebo skupinu zařízení.
* Guest SSID – autentizace pomocí WebAuth pro uživatele (zpravidla pacienty či hosty) s přístupem pouze do internetu. Tito uživatelé si buď sami založí účet (tzv. self-registration portál) nebo jim personál vytvoří účet na AAA serveru.

Součástí cenové kalkulace je kompletní nasazení segmentace počítačové sítě prostřednictvím VLAN, nasazení nového IP plánu a ověřování všech zařízení prostřednictvím AAA serveru. AAA servery v počtu 2ks budou nasazeny v HA režimu.

Licence AAA serveru, pro minimálně 1600 identit, bude funkční, včetně podpory, 5 let od nainstalování tohoto SW.

# Specifikace minimálních požadavků technického řešení

**AAA server – 2ks – pro minimálně 1600 identit**

* On-premise appliance, nepřipouští se cloud řešení
* Licence pro alespoň 1600 současně připojených zařízení
* Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.)
* Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup
* Poskytuje AAA funkce (viz níže)
* S příslušnou licencí podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)
* Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity
* Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace
* Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)
* Je dostupné ve formě Virtuálního stroje na platformách ESX/ESXi, KVM nebo Hyper-V
* RADIUS pro autentizaci, autorizaci, zaznamenávání
* proxy funkce pro externí RADIUS
* PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, TEAP, EAP-FAST
* S příslušnou licencí podpora TACACS+ pro administraci zařízení
* Ověření uživatelů heslem nebo certifikátem
* Ověření MAC adresou připojovaného zařízení
* Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:
  + stavu a typu koncového zařízení (viz níže),
  + uživatele (role, skupiny),
  + místa připojení,
  + historie připojení
* Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě
* Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě
* Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“
* Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat
* Zaznamenávání aktivity uživatelů a zařízení připojených k síti
* Dotazovací systém, korelace záznamů, centralizované výkazy
* Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)
* Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi
* Oprávnění pro hosty přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů
* Samoobslužný portál pro hosty
* Ověření hostů přes HTTP a HTTPS
* S příslušnou licencí automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou
* Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)
* Předdefinované profily pro síťová zařízení NAD od různých výrobců
* Podpora pro IPv6 koncová zařízení
* S příslušnou licencí podpora BYOD:
  + Onboarding (registrace, provisioning, nastavení klientských zařízení)
  + Onboarding/provisioning proces formou samoobsluhu
  + Specifické politiky pro BYOD zařízení
  + Možnost nastavení limitu BYOD zařízení pro jednoho uživatele
  + Interní CA, pro vydávání certifikátů BYOD zařízením
  + Interní CA lze řetězit jako subordinate pod firemní CA
* Možnost autentizace oproti více AD domén, i když nejsou v trust režimu
* Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)
* Podpora Multi-Domain integrace s AD
* Podpora SXP (Exchange Protocol) dle IETF
* Centralizovaná správa
* Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému
* Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení
* Grafické rozhraní pro definici pravidel přístupu k síti
* Grafické rozhraní pro monitorování, definici výkazů, řešení problémů
* Diagnostika problemů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)
* Zaznamenávání událostí na externí syslog server
* Podpora SNMPv3
* NTP pro synchronizaci času
* SMTP pro zasílání zpráv a výstrah přes e-mail
* Centralizované nasazení s podporou vysoké dostupnosti v režimu Active-Active (minimálně 2 servery)
* Appliance podporuje ochranu dat a záznamů