1 Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.
Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.
Součástí dodávky níže uvedených technologií bude i vytvoření virtuálních prostředí, instalace a konfigurace serverových operačních systémů v rámci provedené dodávky technologií, konfigurace doménového kontroleru, DHCP serveru, DNS serveru, souborového serveru; vše do prostředí kupujícího a dle pokynů kupujícího pro informační systémy a prostředí, která dodané technologie budou užívat. Bude se jednat o přizpůsobení pravidel a migraci domény do nového prostředí realizovaného v rámci této dodávky.
Součástí služeb implementace bude dále představení nového prostředí uvedeného do provozu s možností ověření jeho funkčnosti kupujícím a to v oblastech provedené konfigurace zálohování, replikace a obnovy serverů a dat, v oblasti virtualizovaného prostředí serverů a diskové virtualizace a v oblasti publikovaných diskových oddílů.
Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.
Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.
Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.
Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.
Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.
Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.
Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Přepínače, směrovače, přístupové body a sofware pro správu ověřování dle protokolu 802.1x
Nové přepínače a bezdrátová síť budou konfigurovány pro autentizaci připojených zařízení protokolem 802.1X dle níže uvedeného rozsahu.

V neoddělitelném celku s instalovanými aktivními prvky bude dodán a zprovozněn rovněž centrální systém pro ověřování uživatelů pomocí protokolu 802.1x. Systém bude instalován a zprovozněn ve virtuální infrastruktuře zadavatele. Dostatečný výpočetní výkon je zajištěn stávajícími výpočetními prostředky zadavatele. Systém bude zprostředkovávat ověření uživatelů z databáze a na základě příslušnosti ke konkrétním skupinám uživatelů, bude povolovat přístup do lokální sítě. Rovněž bude systém přidělovat zařazení do konkrétních VLAN sítí, na které budou aplikovány filtry a omezení přístupu dle bezpečnostní povahy.

Součástí nasazení výše uvedených technologií bude instalace i migrace stávajících konfigurací a politik ze stávajících přepínačů CISCO a firewallu Kerio Control na zařízení nově dodaná včetně optimalizace takových konfigurací a jejich zdokumentování pro objednatele.

Rozsah implementačních prací pro ověřování dle protokolu 802.1X:

1) Bezdrátová síť
    - Propojení bezdrátové sítě s RADIUS serverem.
    - Propojení RADIUS serveru s AD.
    - Zajištění přístupu uživatelů z AD na zařízeních v AD do interní sítě.
    - Zajištění přístupu uživatelů z AD na zařízeních, která nejsou v AD pouze do Internetu.
    - Implementace SMS brány a propojení s autentizačním portálem pro pacienty.
    - Implementace přístupu pro pacienty s registrací a autentizací na webovém rozhraní (captive portálu).
    - Autentizace přístupových bodů do sítě pomocí 802.1X.
2) Síťové přepínače
    - Konfigurace síťových prvků pro komunikaci s RADIUS serverem.
    - Konfigurace portů pro monitoring přístupu do sítě.
    - Konfigurace portů pro ověřování přístupových bodů pomocí 802.1X
3) Obecné
    - Implementace ověřování managementu síťových prvků přes RADIUS / TACACS+
    - Implementace dalších pravidel přístupu do bezdrátové sítě a konfigurace nekritických portů pro autentizaci 802.1X dle požadavků zadavatele v maximálním rozsahu 20 hodin.

Propojení zařízení – SFP moduly a kabely

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny objednatele, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Dokumentace

Součástí předmětu plnění bude i dodávka dokumentace skutečného provedení, která bude před realizací dodávky předána k odsouhlasení kontaktní osobě objednatele dle kupní smlouvy, na jejímž základě dojde k tomuto plnění. Součástí takové dokumentace musí být uvedení termínů a způsobů provádění jednotlivých dodávek včetně výměna kabeláže. Po provedení dodávky bude tato dokumentace aktualizována na skutečné provedení, včetně grafické vizualizace vybudované síťové infrastruktury a jejího řádného popisu co do konkrétních konfigurací jednotlivých zařízení, jejich typu, jejich funkce v rámci vybudovaného síťového prostředí a způsobu jejich správy.

Součástí dokumentace bude zároveň i konkrétní návod na správu sítě včetně postupů obměny/záměny jednotlivých prvků sítě a dále postupů na připojování a odpojování jednotlivých koncových zařízení. Pro

návrh nové konfigurace sítě musí být respektována, převzata nebo jiným způsobem předpracován pravidla již konfigurovaná v prostředí sítě objednatele.

Součástí dodávky bude návrh a provedení nastavení odpovídajících politik zejména ve formě VLAN sítí a dále konfigurace FW pro potřebu organizace objednatele.

Veškerá dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Předání dokumentace v úplném a řádném rozsahu bude jednou z podmínek akceptace plnění ze strany objednatele.

Uvedení konkrétních označení a názvů

Pokud tyto zadávací podmínky obsahují požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, pak je to z důvodů, že se jedná o stávající zařízení v majetku zadavatele a systémy, se kterými musí být nabízené vybavení kompatibilní. V ostatních případech, pokud by se v některé části ZP takové požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu vyskytly, pak je to z důvodů, že stanovení technických podmínek jiným způsobem nemůže být dostatečně přesné a srozumitelné. V každém takovém případě je v souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, možné nabídnout i jiné, rovnocenné řešení.

Obsah

2 IROP výzva č. 10

2.1 Firewall 2ks

- FW propustnost (1518 bajtů) min 20 Gb/s
- FW propustnost (64 bajtů UDP) min 9 Gb/s
- Počet současných spojení min 2 miliony
- Počet nových spojení min 135 tis./s
- Propustnost IPSec VPN (512 bajtů) min 9 Gb/s
- Propustnost SSL VPN min 900 Mb/s
- Propustnost IPS (HTTP) min 6 Gb/s
- Propustnost IPS (Ent Mix min 2.2 Gb/s
- Propustnost SSL Inspection min 1 Gb/s
- Počet rozhraní GE RJ45 min 18
- Počet rozhraní GE SFP min 4
- Montážní výška max 1RU
- Console port ano
- Vyhrazený management port ano
- USB port ano

Zařízení musí podporovat možnost propojení do HA clusteru v režimu Active-Acive nebo Active-Passive pro zajištění provozu v případě poruchy některého ze zařízení.
Zařízení musí poskytovat další služby, jako je Web filtering, Antivirus, IPS, Application Control.
Záruční servis výrobce v režimu 24x7 zařízení na dobu minimálně 5 let.
Možnost správy zařízení přes konzolu nebo vzdáleně přes zabezpečené webové rozhraní, příkazový řádek nebo specializovanou aplikaci.
Možnost nastavování různých politik pro různé typy provozů a různé skupiny uživatelů.
Možnost základního zobrazení logů a událostí v grafickém rozhraní správy.
Možnost odesílání logů k analýze na specializovaná zařízení.
Součástí dodávky je fyzické instalace stohu výše uvedených firewallu v HA režimu a následná plná integrace do sítě objednatele včetně migrace konfigurace ze stávajícího firewallu.

2.2 Aktivní prvky - přepínače

2.2.1 Páteřní přepínač 2 ks

- L3 přepínač
- 24 SFP+ portu
- volný rozšiřující slot volitelně osaditelný 8x 10 Gbit nebo 2x 40 Gbit porty
- dedikovane stohovaci rozhrani s minimalni propustnosti 480 Gbps pri kruhove topologii
- moznost stohovani az 9 zarizeni
- Out-of-band management port RJ45
- minimalni prepinaci kapacita 640 Gbps
- minimalni forwarding rate 450 Mpps
- osazen nejmene dvema zdroji
- stohovani napajeni mezi jednotlivymi prvky

- modularni (za chodu vymenitelne) ventilatory
- podpora MACSEC
- podpora SDA
- podpora Jumbo Frames (az 9198 bytes)
- podpora SNMPv1, SNMPv2c, and SNMPv3
- podpora standardu IEEE 802.1as, IEEE 802.1s, IEEE 802.1w, IEEE 802.11, IEEE 802.1x, IEEE 802.1x-Rev, IEEE 802.3ad, IEEE 802.1D, IEEE 802.1p CoS prioritization, IEEE 802.1Qat Stream Reservation Protocol, IEEE 802.1Qav, IEEE 802.1Q VLAN
- plnohodnotny CLI management

2.2.2 Přístupový přepínač 9 ks

- L2+ přepínač
- 24 metalickych portu 10/100/1000 a dva SFP+ porty
- dedikovane stohovaci rozhrani s propustnosti az 80 Gbps pri kruhove topologii
- moznost stohovani az 8 zarizeni (plne kompatibilni se stavajicimi prvky rady C2960X)
- Out-of-band management port RJ45
- minimalni prepinaci kapacita 88 Gbps
- minimalni forwarding rate 95 Mpps
- podpora SNMPv1, SNMPv2c, and SNMPv3
- podpora standardu IEEE 802.1D, IEEE 802.1p CoS Prioritization, IEEE 802.1Q, EEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.1ax
- plnohodnotny CLI management

2.2.3 Přístupový přepínač 5 ks

- L2+ přepínač
- 48 metalickych portu 10/100/1000 a dva SFP+ porty
- dedikovane stohovaci rozhrani s propustnosti az 80 Gbps pri kruhove topologii
- moznost stohovani az 8 zarizeni (plne kompatibilni se stavajicimi prvky rady C2960X)
- minimalni prepinaci kapacita 136 Gbps
- Out-of-band management port RJ45
- minimalni forwarding rate 130 Mpps
- podpora SNMPv1, SNMPv2c, and SNMPv3
- podpora standardu IEEE 802.1D, IEEE 802.1p CoS Prioritization, IEEE 802.1Q, EEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.1ax
- plnohodnotny CLI management

2.2.4 Přístupový přepínač 2 ks

- L2+ přepínač
- 24 metalickych portu 10/100/1000 s podporou PoE a dva SFP+ porty
- dedikovane stohovaci rozhrani s propustnosti az 80 Gbps pri kruhove topologii
- moznost stohovani az 8 zarizeni (plne kompatibilni se stavajicimi prvky rady C2960X)

- Out-of-band management port RJ45
- pro PoE k dispozici minimalne 370 W
- minimalni prepinaci kapacita 88 Gbps
- minimalni forwarding rate 95 Mpps
- podpora SNMPv1, SNMPv2c, and SNMPv3
- podpora standardu IEEE 802.3af, IEEE 802.3at, IEEE 802.1D, IEEE 802.1p CoS Prioritization, IEEE 802.1Q, EEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.1ax
- plnohodnotny CLI management

2.2.5 Přístupový přepínač 7 ks

- L2+ přepínač
- 48 metalickych portu 10/100/1000 s podporou PoE a dva SFP+ porty
- dedikovane stohovaci rozhrani s propustnosti az 80 Gbps pri kruhove topologii
- moznost stohovani az 8 zarizeni (plne kompatibilni se stavajicimi prvky rady C2960X)
- Out-of-band management port RJ45
- pro PoE k dispozici minimalne 370 W
- minimalni prepinaci kapacita 136 Gbps
- minimalni forwarding rate 130 Mpps
- podpora SNMPv1, SNMPv2c, and SNMPv3
- podpora standardu IEEE 802.3af, IEEE 802.3at, IEEE 802.1D, IEEE 802.1p CoS Prioritization, IEEE 802.1Q, EEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.1ax
- plnohodnotny CLI management

2.2.6 Příslušenství přepínačů

- vsechny SFP/SFP+ porty pozadujeme osadit moduly SFP+ 10G LR
- soucasti instalace jsou i veskere potrebne opticke kabelaze nutne pro propojeni vyse uvedenych prvku v rezimu 2x 10 Gbit pro kazdou lokalitu/rozvadec; součástí instalace je i napojení na nově dodávanou pasivní infrastrukturu včetně potřebného navařování a dalších služeb souvisejících s nasazením přepínačů na nově dodanou pasivní infrastrukturu a stávající pasivní infrastrukturu objednatele
- součástí dodávky jsou i instalační a konfigurační práce minimalne v nize uvedenem rozsahu:
  - hostname
  - ip adresa, výchozí brána
  - přístupové údaje (dva účty, jeden s plným přístupovým oprávněným, druhý omezený)
  - nastavení přístupů (povolené SSH/SSL, zakázaný telnet/http)
  - nastavení odhlášení uživatele při neaktivitě
  - nastavení snmp (dva účty - read/write, umístění, kontakt)
  - nastavení syslog serveru
  - nastavení času (sntp či ntp synchronizace, časová zóna, letní/zimní)
  - nastavení spanning tree protokolu
  - nastavení syslogu
  - nastavení DHCP snoopingu

- nastavení VLAN a odpovídající nastavení páteřních i přístupových portů
- nastavení linkové agregace optických propojů mezi páteřním přepínačem a přepínači podružnými
- nastavení ochrany proti nechtěnému šíření broadcastu
- popisky důležitých portů (páteřní propoje, servery, AP, kontroler, firewall, atd.)
- vytvoření stohu v lokalitách, kde bude umístěno více aktivních prvků
- nastavení 802.1x, dle již dříve uvedených požadavků

Management software pro přepínače a bezdrátovou síť:

- Virtuální server pro prostředí VMware, které je stávajícím vybavením objednatele
- Požadovaný počet spravovaných zařízení min. 70
- Možnost navýšení počtu spravovaných zařízení formou dokoupení licence
- Kompletní správa životního cyklu infrastruktury (nasazení, administrace, monitoring, odstraňování problémů)
- Grafické web rozhraní pro správu
- Přístup ke GUI i pomocí aplikace pro mobilní zařízení
- Nástroje monitorování, monitorování v reálném čase a odstraňování problémů
- Automatická archivace konfigurací, porovnávání konfigurací, porovnávání konfigurací vůči šablonám
- Konfigurační šablony dle "best practice" a designových příruček
- Inventarizace nasazeného HW v síti
- Inventarizace, nasazení, správa firmware do síťových zařízení
- Monitorování výskytu koncových zařízení, IP telefonů a uživatelů v síti
- Generování reportů bezpečnostních problémů infrastruktury
- Zobrazení L2, L3 topologické mapy
- Kompletní správa životního cyklu bezdrátové sítě (plánování, nasazení, monitoring, troubleshooting, reporting)
- Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí
- Monitoring IPv6 připojení koncových zařízení napříč pevnou i bezdrátovou sítí
- Integrace se znalostní bází výrobce pro usnadnění řešení problémů a správy
- Podpora API pro programatický přístup do databází aplikace správy
- Hierarchické mapy zobrazující umístění AP, šíření signálu a aktuální pozice wifi klientů (notebooků, PDA, WiFi telefonů, WiFi RFID tagů apod.)
- Centrální konfigurace bezdrátových sítí včetně bezpečnostních politik, QoS profilů
- Nástroje pro detekci a řešení problémů v bezdrátové síti (grafy obsazenosti kanálů, grafy odpovídající provozu klientů, atd.)
- Nástroje pro plánování WLAN sítě
- Nástroje pro plánování, nasazení, monitorování a optimalizaci hlasových služeb do bezdrátové sítě
- Podpora SNMPv1, SNMPv2, SNMPv3
- Podpora autorizace a autentizace vůči TACACS+
- Technologický dashboard pro zobrazování výsledků měření kvality signálu bezdrátové sítě
- Zobrazování současných i historických hodnot a trendu kvality signálu bezdrátové sítě

- Zobrazování alarmů týkajících se kvality signálu
- Možnost pokročilého vyhledávání zdrojů interference v bezdrátové síti
- Nástroj pro troubleshooting klientů s funkcí identifikace zdrojů interference, které ovlivňují klienty
- Integrovaný nástroj pro sběr diagnostických dat o kontrolerech a AP v bezdrátové síti
- Automatické dohledání portu pevné sítě s připojeným falešným Access Pointem
- Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení a jednotlivého uživatele v souhrnném pohledu (kontextově) pro rychlejší troubleshooting

2.2.7 Dodávka síťových rozvodů objednatele v souvislosti s nasazením nových aktivních prvků

Současně s nasazením nových aktivních prvků dojde k nasazení nové pasivní části infrastruktury v podobě kabeláže na adrese sídla objednatele ve Strakonicích v rámci areálu uvnitř a mezi budovami nemocnice. Instalace síťových rozvodů bude probíhat za splnění specifických podmínek zanesených v kupní smlouvě s ohledem na skutečnost, že dodávka bude prováděna v nemocničním prostředí za jeho plného provozu.
Objednatel stanovil položkový rozpočet materiálu následujícím způsobem

- 3000m - Optický kabel 24x9/125, SM, OS2 včetně nosného instalačního materiálu zejména žlaby, chráničky, nosné oka pro trasy na klinikách
- 15ks - Optická výsuvná jednotka 19" / 1U pro max. 24 spojek LC/SC
- 26ks - Kazeta pro montáž svárů
- 15ks - Víčko kazety
- 168ks - Spojka LC/PC, SM, modrá
- 336ks - Pigtail LC/PC, 9/125, SM, 1m
- 100ks - Optický patch cord LC/PC-LC/PC, duplex, 2m

K nové pasivní infrastruktuře bude ze strany dodavatele jako dokumentace dodáno následující:

- měření opt.vlákna - výkonové, včetně vystavení protokolu
- Zakreslení tras v objektech do stávající dokumentace nebo v případě potřeby zhotovení zcela nové dokumentace tras dodané pasivní infrastruktury

Za účelem možnosti seznámení s dispozicí areálu objednatele pořádá zadavatel ve lhůtě pro podání nabídek prohlídku místa plnění.
Na pasivní infrastrukturu záruka 5 let s odstraněním závady do 30 dnů v místě dodávky.

2.3 Aktivní prvky - Přístupové body – 17 ks

Minimální funkční požadavky na zařízení:

- Access Point určený pro instalaci na strop/podhled
- Integrované všesměrové antény (v horizontální rovině) pro obě pásma
- Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu, možnost provozovat jedno z rádií v monitorovacím režimu pro 2,4 i 5 GHz současně
- Podpora standardů 802.11a/b/g/n a 802.11ac wave 2
- Podpora 4x4 MIMO, podpora MU-MIMO, až 160 MHz kanál pro 802.11ac
- Minimální počet inzerovaných SSID (BSSID) per radio: 8

- Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 a/g/n/ac klientům (Beam Forming)
- Podpora mechanismů pro přepojení klientů z 2,4GHz do 5GHz pásma a optimalizovaného roamingu
- Access Pointy musí obsahovat X.509 certifikát s lokální platností pro nasazeni PKI
- Hardwarová podpora šifrování řídících i uživatelských dat přenášených mezi AP a kontrolerem, šifrování nesmí mít vliv na propustnost AP
- Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)
- AP uzavřené konstrukce, bez větracích otvorů a ventilátoru
- Access Pointy musí být fyzicky zabezpečitelné/zamknutelné k okolním pevným částem
- Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 a IPv6 pomocí Telnet a SSH
- Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference)
- Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur
- min. 2 x 100/1000 Mbit Ethernet rozhraní
- Napájení AP pomocí 802.3at PoE
- Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům
- Je požadována kompatibilita se stávajícím kontrolerem a jejich společná konfigurace v rámci dodávky plnění – stávající kontroler Cisco CT2504 – včetně případného odpovídajícího počtu licencí pro možnost konfigurace a navázání těchto AP na uvedený kontroler (pro využití s výše uvedeným požadovaným počtem licencí AP objednatel již vlastní licence L-LIC-CT2504-1A v počtu 8 ks, které umožní použití pro výše uvedené požadované AP pro jejich navázání na stávající kontroler)
- Součástí dodávky jsou i níže uvedené implementační a konfigurační práce:
    - Integrace nových přístupových bodů ke stávajícímu kontroleru
    - Konfigurace nového SSID pro pacienty s politikou proti novému RADIUS serveru
    - Konfigurace nového SSID pro uživatele v AD (politika řešena na novém RADIUS serveru)
    - Konfigurace příslušných firewallových pravidel či potřebných VLAN
    - Konfigurace nového SSID s politikou WPA2/AES a autentizací pomocí PSK. PSK musí být definovatelné na MAC adresu či skupinu MAC adres dle politiky na novém RADIUS serveru.
    - Úprava konfigurace dle best practices s novými přístupovými body.

2.4 Aktivní prvky – síťový software

Předmětem dodávky je softwarová funkcionalita k výše uvedeným aktivním prvkům, která zajistí v rámci dodávky v prostředí objednatele zabezpečení minimálně v oblasti 802.1x, návštěvnických sítí a vnesených zařízeních.

2.4.1 Software pro zabezpečení 802.1x nad dodanými aktivními prvky

Je požadován centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (zejména uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení).

Minimální požadavky na funkcionalitu:

- Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) software bude poskytovat ochranu před neoprávněným přístupem k síti LAN, bezdrátové síti WiFi (metodou 802.1x) a pro VPN přístup.
- Software bude poskytovat funkce a služby ověřování, autorizace a záznamů o průběhu připojení uživatelů a zařízení k síti.
- Umožní klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)
- Umožní centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity
- Umožní snadné zálohování, rychlou a úplnou obnovu konfigurace
- Musí být dostupný ve formě tzv. appliance (hardware i software podporovaný jedním výrobcem)
- požadované podporované protokoly
    - RADIUS pro autentizaci, autorizaci, zaznamenávání
    - proxy funkce pro externí RADIUS
    - PAP, MS-CHAP, MS-CAHPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST
    - podpora TACACS+ pro administraci zařízení
- požadované podporované databáze uživatelů s možností definovat pořadí průchodu
    - interní (pro uživatele a koncová zařízení)
    - Active direktory
    - LDAP (RFC 2251)
    - RADIUS Token identity source (RFC 2865)
    - RSA RADIUS token server
    - Certificate authentication profile
- požadavek na možnosti ověřování uživatelů a zařízení
    - ověření uživatelů heslem nebo certifikátem
    - ověření MAC adresou připojovaného zařízení
- požadovaná funkcionalita v oblasti autorizace – pružný systém pro definici pravidel pro přístup k síti
    - řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle
        - stavu a typu koncového zařízení
        - 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 přístupu i možným zapojením do trasy komunikace autorizovaných zařízení
  - podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů
  - možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti
  - řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat
- požadovaná funkcionalita v oblasti Accoutning
  - zaznamenávání aktivity uživatelů a zařízení připojených k síti
  - obsahuje dotazovací systém, korelace záznamů, centralizované výkazy
  - obsahuje systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému ověřování, autentizace a autorizace, dostupnost externích databází, aktivita filtrů)
- řešení musí umožnit rozpoznávání typu koncových zařízení
  - automatické rozpoznávání a klasifikace připojených zařízení (zejména PC, telefonů, tabletů, mobilních telefonů) 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 vendorů
  - podpora pro IPv6 koncová zařízení
- další požadované vlastnosti řešení
  - možnost autentizace proti více AD doménám, 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
- požadované funkce pro správu ověřovacího systému
  - centralizovaná správa
  - definice rolí administrátorů a úrovní přístupů k ověřovacímu systému
  - zjednodušení správy vytvářením skupin uživatelů, koncových a síťových zařízení
  - grafické rozhraní pro definici pravidel přístupu k síti
  - grafické rozhraní pro monitorování, definici výkazů, řešení problémů
  - diagnostika problémů (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 prostřednictvím emailu
- další požadované technické parametry
  - centralizované nasazení s podporou vysoké dostupnosti
  - možnost nasazení ve virtuálním prostředí objednatele s podporou VMwre ESXi 5.x a 6.x nebo KVM na Red Hat 7.x

- podpora výrobce software v délce 1 rok spočívající zejména v nárocích na opravné verze software a jeho zabezpečení, která bude uhrazena současně s dodávkou

2.4.2 Software pro řízení Guest sítí nad dodanými aktivními prvky – minimálně pro 100 zařízení současně

Minimální požadavky na funkcionalitu:

- vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, pacienty, externí spolupracovníky apod. ve fixních LAN i WiFi
- oprávnění umožní přidělování správcem přístupu prostřednictvím portálu pro snadné vytváření dočasných účtů
- musí obsahovat samoobslužný portál pro uživatele
- musí umožnit ověření prostřednictvím HTTP a HTTPS

Příslušenství pro provoz Guest sítí

- součástí systému pro řízení Guest sítí bude i SMS gateway pro zasílání hesla ze samoobslužného systému pomocí SMS
- tato brána bude mít minimálně tyto parametry:
    - hardwarové provedení
    - minimálně 2 neblokované GSM moduly (umožní provoz min .2 aktivních SIM karty)
    - Emal2SMS nebo HTTP API včetně potřebných licencí pro alespoň 5 uživatelů
    - min. 1x Ethernet port
    - externí anténa
    - možnost blokovat/povolit konkrétní předčíslí či maskování telefonního čísla
- podpora výrobce software v délce 1 rok spočívající zejména v nárocích na opravné verze software a jeho zabezpečení, která bude uhrazena současně s dodávkou

2.4.3 Software pro management firemních a BYOD zařízení nad dodanými aktivními prvky – minimálně pro 500 zařízení

Minimální požadavky na funkcionalitu:

- onboarding (registrace, provisioning, nastavení klientských zařízení)
- onboarding/provisioning proces formou samoobsluhy
- možnost nastavení specifické politiky pro BOYD zařízení
- možnost nastavení limitu BOYD zařízení na jednoho uživatele
- interní CA pro vydávání certifikátů BOYD zařízením
- interní CA, která musí umožnit její řetězení formou subordinace pod firemní CA
- podpora výrobce software v délce 5 let spočívající zejména v nárocích na opravné verze software a jeho zabezpečení, která bude uhrazena současně s dodávkou

2.5 Síťové úložiště

Minimální funkční požadavky na zařízení:

- síťové diskové úložiště s možností instalace 12 ks 3,5“ disků SATA i SAS v základní jednotce, s možností rozšíření o další přídavné police
- podpora běžných typů Raidů (Raid 10, 5, 6) a funkce Hot Spare

- provedení rack s dvojicí redundantních zdrojů
- Výkonný CPU (minimálně 6 jader) a 32 GB RAM DDR4 s možností dalšího rozšíření
- 2 PCI-E pozice pro přídavné karty
- Konektivita min. 4 x 1 GbE, 2 x 10 GbE – obě s podporou funkce síťové agregace nebo failover
- podpora systému souborů: EXT4, EXT3, NTFS, FAT, HFS+, exFAT
- kompatibilita se stávajícím prostředím objednatele minimálně VMware vSphere a Windows Server 2012 a R2
- maximální velikost jednoho svazku 200 TB
- osazeno „fyzickou" diskovou kapacitou min. 120 TB, 120 TB je bráno jako součet kapacit všech disků bez vytvořeného Raidu
- záruční servis 5 let na celý systém síťového úložiště NBD on-site
- Instalace a konfigurace NAS (včetně vytvoření vhodné raid konfigurace); montáž NAS do racku, připojení k UPS a konfigurace automatického korektního vypnutí a startu systémů, připojení do LAN, instalace aktuálních verzí firmware, konfigurace managementu a vzdálené správy, nastavení e-mailových notifikací při kritické události; vytvoření diskových oddílů, jejich publikace produkčním serverům pro ukládání replika a záloh virtuálních serverů dle pokynů objednatele
- Součástí dodávky síťového úložiště bude i jeho konfigurace zálohování a dále konfigurace doménového prostředí stávajícího Windows serveru, v rámci nějž budou osobní složky uživatelů přesunuty nebo online replikovány (synchronizováno) do předmětného síťového úložiště. V prostředí objednatele tak dojde k zajištění dostupnosti uživatelských dat v rámci prostředí organizace objednatele a dále dojde ke sjednocení zálohování osobních složek uživatelů v rámci jednotného diskového prostoru na předmětném síťovém úložišti, při zachování řízení přístupových oprávnění k samotnému obsahu těchto složek.

2.5.1 Zálohovací software pro síťové úložiště

Obecné požadavky na funkcionalitu software

- Zálohovací software podporuje infrastrukturu VMware založenou na verzích vSphere 4.1, 5.0, 5.1, 5.5, 6.0 a Hyper-V 2012 a Hyper-V 2012 R2 (podpora *.vhdx). Všechny níže popsané funkcionality musí být splněny pro všechny zmíněné verze hypervizorů.
- Software podporuje ESXi servery spravované pomocí VMware vCenter Serveru a samostatné ESXi servery.
- Software podporuje Hyper-V servery spravované System Center Virtual Machine Managerem, Hyper-V servery ve failover clusteru a samostatné Hyper-V servery
- Software musí podporovat zálohu všech operačních systémů, které jsou podporované pro provoz ve VMware nebo Hyper-V
- dodaný software musí být licenčně pokryt jako celek na výše uvedené diskové úložiště a níže požadované funkcioanlity tak, aby nebylo potřeba dokupovat žádné jeho další komponenty
- software nesmí být svázán s konkrétním hardware a musí umožnit využití na jakémkoliv serveru a diskovém úložišti
- Software musí vytvářet soubory záloh, které je snadné přesouvat a jsou nezávislé na metadatech a databázi s možností nastavení vytváření těchto souborů na principu per backup / per VM.

- Software musí disponovat deduplikačním a kompresním mechanismem, který zaručí redukci diskového prostoru potřebného pro zálohovací soubory. Tato funkcionalita nesmí mít dopad na žádnou z níže požadovaných vlastností.
- Software musí podporovat abstrakční vrtstvu pro vytváření škálovatelného zálohovacího repository (single virtual pool) složeného ze třech extentů.
- Software nesmí využívat centrální databázi pro ukládání deduplikačních metadat. Ztráta databáze nesmí vést k nemožnosti obnovy dat ze zálohovacích souborů. Deduplikační metadata měla být uložena s backup soubory.
- Software nesmí instalovat žádný typ stálého agenta uvnitř virtuálního stroje, který vyžaduje údržbu, instalaci, udržování aktualizací atd.
- agent instalovaný ve VM by neměl být potřeba pro proces zálohy a obnovy.
- Software musí využívat „single pass backup" – s možnosti vyjmutí adresářů / souborů z procesu zálohy. „Single pass backup" je vyžadován pro všechny druhy obnov, včetně granulárních obnov.
- Software musí mít mechanismus pro notifikaci průběhu záloh a chybách pomocí email nebo SNMP
- Software musí umožnit definici pre- a post- backup skriptu a pre-freeze / post-thaw skriptu (vmware)
- Software musí podporovat přímou integraci s VMware vCloud Director 5.1, 5.5, 5.6 a archivovat vCD metadata
- Software musí podporovat obnovu Virtuálních Serverů přímo do prostředí VMware vCloud Director
- Software musí umožnit zálohu konfigurace celého zálohovacího prostředí pro případ reinstalace nebo migrace v případě potřeby.
- Software musí podporovat enkrypci celé síťové komunikace mezi všemi komponentami řešení bez dopadu na níže popsané funkcionality.
- Software musí podporovat enkrypci zálohovacích souborů bez dopadu na níže popsané funkcionality.
- Software poskytuje správu klíčů a možnost obnovy v případě ztráty hesla k šifrovanému zálohovacímu souboru
- Software musí umožňovat zálohování Hyper-V shared *.vhdx disků.
- Software musí mít klient/server architekturu s možností instalace více instance administrátorské konzole.

<u>Požadavky na funkcionalitu v oblasti obnovy dat ve vztahu k předmětu zálohy</u>

- Software musí využívat Change Block Tracking (CBT) pro oba podporované hypervisory VMware a Hyper-V. CBT technologie měla být certifikována výrobcem hypervisoru.
- Software musí poskytovat technologii pro omezení stresu na produkční datové úložiště v průběhu zálohování v případě, že process zálohování vede ke zvýšení latence datového úložiště. Tato vlastnost musí být dostupná pro oba podporované hypervisory.
- Software musí poskytovat automatickou detekci "orphaned snapshots" a měl by automaticky zajistit konsolidaci takových snapshotů
- Software musí mít možnost vytváření archivů záloh na páskové knihovny s podporou trackování VM na páskách

- Páskovou knihovnu mělo být možné provozovat separátně od backup serveru
- Software musí podporovat vytváření vzdálených kopií záloh
- Software musí podporovat vytváření a správu GFS (Grandfather-father-son) retenční politiky
- Software musí využívat výhod protokolu EMC DDBOOST v případě použití EMC DataDomain jako backup repository
- Software musí využívat výhod protokolu Catalyst v případě použití HP StoreOnce jako backup repository. Technologie musí být podporována pro síťový i FibreChannel přístup.
- Software musí disponovat schopností kopírovat body obnovy a replikovat VM do vzálené lokality
- Software podporuje funkcionalitu replikace VM functionality mezi ESXi server včetně asynchronní kontinuální replikace.
- Výše zmíněná funkcionalita musí být dostupná i pro prostředí Hyper-V
- Zálohovací soubory musí být možné využít jako zdroj pro replikaci VM
- Software musí uchovávat více restore pointů replikovaných VM.
- Software musí umožnit "seeding" repliky z existující VM.
- Software musí podporovat všechny zálohovací transportní režimy podporované hypervisorem (network, hotadd, direct SAN, direct NFS)
- Software podporuje možnost vytvářen „ad-hoc" záloh pomocí nativního klienta, nebo pomocí vSphere web klienta
- Proces zálohy musí podporovat paralelní zpracování VM a jejich virtuálních disků.

<u>Požadavky na funkcionalitu v oblasti obnovy dat v čase</u>

- Software musí umožňovat okamžitou obnovu vice virtuálních strojů bez nutnosti kopírování dat na produkční datové úložiště z libovolného bodu obnovy.
- Podobná funcionalita musí být dostupná také pro prostředí Hyper-V
- VM spuštěná v režimu okamžité obnovy musí umožňovat migrovat on-line s využitím vlastností hypervisoru. V případě, že hypervisor tuto technologii nepodporuje, software musí využít vlastní technologii pro online migraci
- Software podporuje obnovu celé VM, souborů VM, nebo virtuálních disků VM.
- Software musí umožnit obnovu souborů k operátorovi, nebo přímo do VM běžící v produkci
- Obnova souborů VM musí být prováděna buď s použitím síťového přístupu, nebo VIX API v prostředí VMware
- Je požadována podpora min. následujících souborových systémů:
    - Linux - ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS
    - BSD - UFS, UFS2
    - Solaris - ZFS
    - Mac - HFS, HFS+
    - Windows - NTFS, FAT, FAT32, ReFS
- Software musí umožňovat okamžitou granulární obnovu aplikačních položek bez nutnosti instalovat agenta do VM.
- Musí podporovat granulární obnovu Active Directory (jakýkoliv object, jakýkoliv atribut, obnova uživatelského účtu včetně hesla, GPO, AD configuration Partition),

- Musí podporovat granulární obnovu Microsoft Exchange 2010 a novější (jakýkoliv objekt včetně objektů z adresáře „Permanently Deleted Objects",)
- Musí podporovat obnovu Microsoft SQL 2005 a novější (database s možností point-in-time recovery, obnova na úrovní tabulek a schémat)
- Musí podporovat obnovu Microsoft Sharepoint Server 2010 a novější (full site recovery, objekty a položky uložené v SharePoint serveru).
- Software musí podporovat granulární obnovu databází Oracle běžících nad Linux a Windows OS (obnova v režimu point-in-time, obnova tabulek)
- Výše zmíněné funkcionality nesmějí vyžadovat obnovu celého Virtuálního Stroje nebo jeho zapnutí.
- Software musí umožňovat indexaci souborů z Microsoft Windows a Linux VM, která poskytuje rychlé vyhledávání souborů ze záloh
- Software musí využívat mechanismus VSS zabudovaný v Microsoft Windows OS vždy, když je to možné.
- Software musí umožnit obnovu VM z hardware snapshot z podporovaných diskových polí.
- Software musí podorovat „reverse CBT" a direct SAN obnovy

Požadovaná funkcionalita v oblasti předcházení rizik

- Software musí poskytovat možnost vytvářet izolované prostředí proVMware a Hyper-V infrastrukturu spouštěním VM přímo ze zálohy. Pro prostředí VMWare musí nabízet vytvoření izolovaného prostředí přímo ze snapshotu podporovaného diskového pole.
- Software musí mít mechanismus pro ověřování záloh, umožňující testování obnov VM v izolovaném prostředí pro VMware a Hyper-V. Verifikace musí být možné spouštět v časovém plánu a musí být plně automatizované.
- Podobný mechanismus musí být podporován i pro replikované VM (VMWare).

Podpora software

- podpora výrobce software v délce 5 let spočívající zejména v nárocích na opravné verze software a jeho zabezpečení, která bude uhrazena současně s dodávkou

2.6 Tokeny - 100 ks

Minimální požadavky na funkcionalitu:

- zařízení určené k přenosu a práci s kvalifikovanými certifikáty
- zařízení musí být vybaveno USB konektorem typu A a podporovat verzi min. USB 2.0
- zařízení musí umožnit správu certifikátů, které na něm mají být bezpečně uloženy
- zařízení musí umožňovat obměnu certifikátů ve svém úložišti
- zařízení musí umožňovat podporu vedení evidence jednotlivých tokenů
- je požadována dodávka zařízení kompatibilních se stávající certifikační autoritou nemocnice tedy PostSignum České pošty s.p.
- s certifikáty výše uvedené certifikační autority musejí tokeny zabezpečit dodržení Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (Nařízení eIDAS) a dále všech odpovídajících prováděcích národních právních aktů k tomuto nařízení, zejména zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění

- podporovaný operační systém min. Windows 32/64 bit ve verzi 7, 8.1, 10, Server 2008, Server 2008 R2
- standardy min. EN 60950/IEC 60950, ISO-7816, PC / SC, CE, FCC, RoHS, VCCI, CCID, Microsoft WHQL, EMV, PKCS#11 v2.11, Microsoft CAPI, TokenD, PC/SC, X.509 v3, SSL v3, IPSec
- podpora šifrovacích algoritmů min. AES-128, DES, 3DES, RSA
- hashovací funkce min. SHA-1, SHA-256
- podporovaná velikost klíče min. 2018 bitů
- požadovaná životnost min. 100.000 cyklů čtení/zápis
- zařízení musí umožňovat jednoduché a časté přenášení a zapojování do USB portů
- záruka k zařízení bude požadována v délce 2 let s opravou v místě dodávky do 30 dnů ode dne nahlášení vady zařízení