## Příloha č. 2 – Technická specifikace

# POPIS SOUČASNÉHO STAVU

Současná infrastruktura pro společnou VT obsahuje systém serverů HP Blade c7000 s FC switch Brocade 8-16Gb, PassThru modul 1GbE a 10GbE switch 1:10, servery BL460c Gen 7-10, několik diskových polí různých generací (HP MSA 2012fc, HP MSA 2040, HPE 3Par 8200) a několik zdrojů zálohovaného napájení (Eaton PW9130i3000R).

Rozmístění do několika lokalit umožnilo částečné zlepšení dostupnosti (všechny klíčové služby pro autonomní běh jsou umístěny v dané lokalitě) i zlepšení bezpečnosti dat (zálohování do druhé lokality).

Klíčovou vlastností systému je možnost fyzického přenosu serverů i úložišť (interních i disků) mezi lokalitami, a tak lepší zabezpečení i optimalizace.
Pro běh všech primárních služeb využívá fakulta operační systémy Microsoft Windows 2012 R2 a 2008 R2 Server s nadstavbou Hyper-V a souborem aplikací Microsoft Systém Center 2012 R2.

Většina primárních aplikačních serverů využívá programové vybavení Microsoft, takže ve spojení s uživatelskými počítači na bázi Microsoft Windows 10 a Microsoft Office je celé prostředí prakticky homogenní. To významným způsobem usnadňuje správu i nasazování nových aplikací třetích stran, což se příznivě odráží v nízkých provozních nákladech.

Zadavatel požaduje zejména s ohledem k nákladům na integraci i správu v maximální možné míře zachovat homogenitu systému. Proto požadujeme technické vybavení plně kompatibilní se stávajícím HW a SW vybavením, které plnohodnotně doplní stávající provozovanou infrastrukturu.

Dále zadavatel provozuje jako hlavní FW jako pro ochranu perimetru Sophos UTM9 FW verze 9.707 (s volbami Base Functionality, Network Protection, Endpoint AntiVirus) s jen jednou virtuální instancí v rámci systémového prostředí HP blade serverů a Microsoft Hyper – V, který chrání perimetr mezi veřejným internetem/intranetem a DMZ zónou. Mimo to jsou historicky provozovány dva Microsoft Forefront Threat Management Gateway jako interní FW pro bezpečné oddělení interních sítí intranetu a několika částí studentského segmentu datové sítě. Bezdrátové sítě jsou odděleny dalšími samostatnými FW.

Toto stávající řešení FW bylo koncipováno jako dočasné a tedy neredundantní, virtualizované s minimálními náklady na pořízení, správu a bez dodatečných investic s výhledem na jeho náhradu po přestěhování organizace zadavatele do nové budovy UNIMEC II.

Oba výše uvedené FW tedy považuje zadavatel za zastaralé ať už z pohledu užitnosti nebo provedené implementace a jejich možností provozu. Z tohoto důvodu zadavatel neklade podmínku na jakoukoli kompatibilitu nebo rozvoj stávajícího řešení.
Zadavatel přepokládá migraci stávající konfigurace min. ve stejném rozsahu funkcionality, viz dále popis budoucího stavu.

Rámcové parametry současného stavu:

- Dvě plně redundantní linky do internetu vedené přes optickou infrastrukturu města Plzně do sítě CESNET. Cesty jsou routovány pomocí BGP protokolu s automatickým přepínáním na sekundární linku v případě výpadku linky primární a zpět
- Segmentace sítě na intranet / internet / dmz
- Filtrovací a forwardovací pravidla v počtu cca 50 pravidel FW a 10 pravidel SNAT (Sophos) + 140 pravidel FW (MS TMG)
- Zabezpečená VPN s možností využívat ověření pomocí Active Directory ve správě zadavatele a s možností generování konfigurace instalační sady pro klienta
- Intrusion detection systém
- DST nat pravidla pro vzdálený přístup z internetu do internetu v počtu 170 pravidel DNAT včetně filtrovacích (Sophos).

# POPIS CÍLOVÉHO STAVU

Tato kapitola obsahuje závazné technické, servisní a záruční požadavky Zadavatele na plnění veřejné zakázky formou dodávky těchto zařízení, které musí Uchazeč plně respektovat při zpracování nabídky. Dodávané technické i programové vybavení musí být nové, a tedy nepoužité, s kompletním příslušenstvím, bez známek poškození nebo neodborného zacházení, a splňující podmínky poskytnutí záruky podle předepsaných pravidel výrobce.

Podpora a servis těchto zařízení musí být organizačně zajištěna prostřednictvím výrobce nebo jeho pověřeného zástupce. Pro potvrzení si zadavatel vyhrazuje právo ověřit sériová čísla dodaného zboží přímo u výrobce již v rámci dodávky.

Záruka musí obsahovat bezplatnou dodávku náhradních dílů, bezplatné servisní práce a zahrnovat veškeré související služby a dodávky, zejména dopravu na místo a z místa instalace, apod. Pokud není náhradní díl standardně uživatelsky výměnný, je součástí těchto prací i jeho odborná záměna výrobcem vyškoleným technikem.

Nabídka musí obsahovat úplný výčet zařízení a jejich dílčích částí s přesným obchodním označením výrobce (objednací kód) a cenou.

Z důvodu zastřešení technického vybavení společnou formou podpory a garantované vzájemné kompatibility požadujeme, aby veškeré dodávané komponenty serverové infrastruktury, SAN infrastruktury, pásková knihovna a primární diskové pole byly od stejného výrobce, nové, nepoužité, z oficiální distribuce výrobce určené pro Českou republiku.
Pokud bude nezbytné dodat drobné komponenty OEM (např. SPF transcievery do datových přepínačů), je požadována plná kompatibilita se zařízením garantovaná uchazečem a sjednocená forma podpory i pro tyto dodávané komponenty. OEM prvky je možné dodat pouze tam, kde je to v rámci následující specifikace explicitně uvedeno. Jinak se přepokládá užití prvků pouze garantovaných výrobcem zařízení.

Součástí dodávky je i instalace na místo určení, prověření funkčnosti a oficiální potvrzení výrobce (nebo jeho oficiálně pověřeného tuzemského zástupce) o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení – dodací list) pro český trh a koncového zákazníka. Dále zadavatel požaduje oficiální potvrzení výrobce (nebo jeho oficiálně pověřeného tuzemského zástupce) o registraci licencí, poskytnutí podpory i záruk dodávaných zařízení a jejich součásti v souladu s uvedenými požadavky.
Potvrzení výrobce (nebo jeho oficiálně pověřeného tuzemského zástupce) není třeba v případě samostatně dodávané kabeláže a příp. OEM drobných komponent a dalšího instalačního materiálu.

Předmětem plnění veřejné zakázky na dodávky je dodávka, instalace a zprovoznění serverové infrastruktury, diskových polí, firewallu, propojovací kabeláže a dalšího příslušenství (dále jen technické vybavení) pro instalaci do serverovny nové budovy zadavatele UniMeC II (dále jen primární serverovna). Technické vybavení bude dodavatelem dodáno na místo a instalováno do připravených rozvaděčů RACK (druhé podzemní podlaží) a příp. v rámci dodržení lokalitní topologie a redundance zálohování a bezpečné správy i na jiná dále specifikovaná umístění. Serverovna i další prostory jsou plně vybavené pro instalaci požadovaného technického vybavení stran napájení, chlazení a prostorového umístění. K dispozici bude i komplexní dále specifikovaná infrastruktura datové sítě.
V rámci instalace zadavatel požaduje odbornou instalaci technického vybavení do Rack rozvaděčů. Je požadováno zprovoznění veškerého technického vybavení, zejména pak:

- Fyzická instalace a kompletní služba zprovoznění, SW instalace a začlenění do provozního prostředí zadavatele certifikovaným technikem výrobce
- Zadání všech nezbytných licenčních klíčů dodávaného technického vybavení a operačních systému, aktivace všech požadovaných funkcionalit v plném rozsahu v souladu s technickou specifikací.
- Propojení a konfigurace LAN a SAN sítě.
- Konfigurace technického vybavení, aktivace v centrálním managementu

- Propojení a konfigurace SAN do stávající serverovny budovy Biomedického centra, kde je umístěná druhá serverovna (dále jen sekundární serverovna). Zadavatel zajistí propojení serveroven pomocí min. 12x optický kabel SM se zakončením konektorem E2000
- Rozšíření stávajícího diskového pole se stávajícím polem HPE 3Par 8200 viz specifikace dále (kapitola 3.2) a zajištění replikace mezi nově dodaným a původním diskovým polem pro zajištění datové lokalitní redundance.
- Nastavení funkcionality replikace diskových polí
- Nastavení zálohování a zálohovací jednotky
- Instalace a nastavení nástroje společné správy žiletkových serverů, jejich profilů, storage infrastruktury a kapacity pro jednotnou správu zdrojů
- Konfigurace firewallu jako plnohodnotnou náhradu stávajícího řešení na platformě Sophos (dle kapitoly 5), vč, migrace všech implementovaných pravidel, filtrů a dalších funkcionalit
- Ověření vysoké dostupnosti a odolnosti proti výpadku datových linek do internetu
- Zaškolení obsluhy

Součástí plnění je poskytnutí uživatelské podpory, jejíž rozsah je definován čl. VII Kupní smlouvy.

Z důvodu snazší správy a požadavků na spolehlivost musí všechny firmware dodávané technického vybavení, operační systémy a programy i SW dohledové a management nástroje být součástí dodávky řešení a to v poslední verzi vydané výrobcem k času předání zboží, s časově neomezenou licencí a nárokem na nové verze minimálně po dobu 60 měsíců.

# Technické požadavky

## 1) Serverová infrastruktura

Serverová infrastruktura s předpokládaným umístěním do primární serverovny ve formě žiletkového šasi, s jednoduchou konvergovanou správou všech serverových a infrastrukturních komponent a nastavení, serverových a storage profilů a společnou správou server a storage infrastruktury, dle následujících požadavků. Šasi bude osazeno minimálně 4x serverem dle následujících požadavků.

V sekundární serverovně zadavatel nepožaduje rozšíření serverové infrastruktury – zde v rámci ochrany investic bude s výhodou použito stávajících zdrojů na stávajícím blade šasi.

### 1.1 Serverové Šasi

**Hardwarová specifikace Šasi**

- musí splňovat následující minimální požadavky:
  - Blade šasi pro serverovou infrastrukturu a konvergovanou interní síťovou konektivitu SAN i LAN s podporou virtualizace
  - Šasi s možností instalace minimálně 12ks blade žiletkových serverů
  - veškeré aktivní komponenty v šasi musí být redundantní
  - podpora poskytování fyzické, virtuální i kontejnerové infrastruktury s mixem dostupných výpočetních, úložných a síťových prostředků.
  - montáž do 19“ racku, výška šasi maximálně 10U
  - dvě redundantní konvergovaná síťová zařízení s možností rozšíření o další dva redundantní páry switchových modulů
  - dva redundantní management moduly s oddělenou sítí pro správu a produkční síť, každý modul požadujeme osadit páry 10Gb optických SR modulů s patch kabely pro připojení k externím management switchům
  - jednofázové integrované napájecí zdroje ve formě hot-plug vyměnitelné za provozu, osazeno minimálně napájecími zdroji N+1 s nejvyšším dostupným výkonem pro nabízené šasi a s účinností minimálně ve třídě Platinum.
  - redundantní hot plug ventilátory, v maximální konfiguraci (plně osazené ventilátory). Směr chlazení šasi musí probíhat zepředu dozadu s ohledem na připravené podmínky v serverovně zadavatele.

- I/O porty minimálně:
  - LAN a SAN vyvedené zcela redundantně ze serverů do páteřních switchů LAN/SAN (minimálně dva aktivní konvergované prvky)
  - každý prvek musí podporovat zdvojené 50Gb downlinky k blade serverům s podporou rozdělení každého portu na minimálně 8 uživatelsky definovatelných částí
  - možnost osazení každého prvku alespoň 6x externí QSFP28 port, všechny s podporou 1x 100Gb, 4x25Gb, 1x40Gb, 4x10Gb Ethernet, nebo 1x32Gb FC.
  - každý prvek je třeba osadit 1x 100Gb Ethernet QSFP28 kabelem 3m délky, 2x 40Gb Ethernet QSFP+ Bidirectional transceiverem s LC interface a 2x 32Gb SFP+ FC SAN optickým SW transceiverem s příslušnou redukcí z QSFP28 portu
  - pro každý prvek požadujeme dodat rovněž dva 40Gb bidirectional QSFP+ transceivery plně kompatibilní s infrastrukturou páteřních přepínačů (Aruba CX8325) a příslušnou kabeláž 10m délky, pro připojení daného šasi/prvku k páteřní infrastruktuře. Z důvodu zachovaní kompatibility a podpory hospodářské soutěže mohou být požadované transceivery pro páteřní přepínače i OEM. Jejich plnou kompatibilitu a bezproblémové fungování v infrastruktuře zadavatele garantuje uchazeč.

**Funkční specifikace Šasi**

- správa z jediné centrální konzole, s konfiguraci výpočetních a síťových prostředků, volbou lokálního úložiště typu DAS, či externího úložiště FC SAN včetně jeho správy (dodané diskové SAN úložiště musí být s touto formou správy plně kompatibilní a plně spravovatelné)
- centrální konzole s jednotným API pro integraci do obvyklých nástrojů pro správu, MS SystemCenter ev. VMWare vCenter i do OpenSource nástrojů jako je Chef, Ansible, Docker a OpenStack.

- možnost tvorby softwarově definovaných šablon serverů pro standardizaci prostředků v rámci prostředí a provádění rychlých změn v infrastruktuře. Šablony musí obsahovat definici standardu minimálně pro serverový BIOS, verzi firmware, síťovou konfiguraci infrastruktury, bootovací zařízení, nastavení RAID či připojení diskového prostoru z nabízeného externího úložiště.
- možnost skriptování pro opětovné přiřazení výpočetních zdrojů různým pracovním prostředím, tedy opětovně poskytnout výpočetní, síťové a kapacitní zdroje z jednoho pracovního prostředí do jiného.
- pro zvýšení odolnosti proti selhání propojení je vyžadována podpora agregace modulů (MLAG)
- schopnost agregace více šasi pro konsolidaci síťových připojení datového centra
- agregace schopná zahrnout minimálně 36 serverů (3 šasi) bez negativního vlivu na rychlost uplink a downlink portů.
- Layer2 provoz přepínaný v rámci agregace police bez nutnosti použití Top of Rack přepínačů
- přepínací latence Ethernet mezi policemi v rámci agregace šasi nesmí překročit jednu mikrosekundu
- možnost propojení minimálně 3 šasi do jednotného okruhu s centrální správou všech zdrojů v připojených šasi
- lokální připojení k šasi přes DisplayPort a USB konektory, případně dodanou přechodkou
- pokud jakákoliv výše uvedená funkčnost vyžaduje licenci, požadujeme dodání všech potřebných licencí pro plně osazené šasi a neomezenou kapacitu.

**Požadavky na správu Šasi**

- pro zajištění kompatibility musí být software pro správu od stejného výrobce jako nabízené šasi a nabízená storage, a musí být schopen spravovat všechny součásti (servery, konvergovanou infrastrukturu, šasi, SAN a SAN storage)
- software zprovozněný a využívající zdroje přímo v šasi, v rámci redundantního fyzického zařízení pro správu - ve více připojených šasi s plnou podporou převzetí služeb při selhání a s vysokou dostupností
- schopnost vyhledat automaticky výpočetní, úložné a síťové prvky v šasi nebo v celém jednotném řídícím okruhu
- zobrazování informací o napájení, zdraví, aktivitách jednotlivých částí šasi, DAS úložiště a I/O modulů
- správa a definice softwarově definovaných profilů výpočetních, storage a síťových zdrojů a jejich přiřazení pracovním prostředím. Možnost definice profilů předem (bez navázání na daný server) a možnost aplikace profilu na jiný server či na prázdný serverový slot pro přípravu na rozšíření.
- aktualizace firmwaru a ovladačů operačního systému v rámci profilů
- uživatelské rozhraní s mapováním fyzických prostředků skrze logické zdroje, s chytrým vyhledáváním libovolných parametrů napříč celým prostředím, logováním aktivit, s možností mobilního přístupu, v HTML5.
- přehledná správa v rámci definovatelného dashboardu
- správa po dedikované management síti 10GbE nebo vyšší (pro komunikaci mezi více šasi), zcela odděleně od produkční datové komunikace
- reporting aktivit a inventarizace zařízení v blade šasi, zobrazení a reporting informací o napájení a chlazení, využití napájení pro server a pro šasi v reálném čase. Možnost exportu reportů do csv a MS Excel
- správa zahrnující interní a externí storage provisioning pro lokální a SAN úložiště, pomocí jednotného nástroje - viz části SAN infrastruktura, Disková pole
- přiřazení privátního a sdíleného úložného prostoru z nabízeného diskového pole SAN k profilům serverů
- boot from SAN podpora pro Fibre Channel, Fibre Channel over Ethernet a iSCSI
- součástí musí být integrační balíčky a případné licence pro napojení na VMware vCenter 6.5 a vyšší, Microsoft System Center a nástroje DevOps jako Chef, Ansible, Docker a OpenStack.

## 1.2 Servery

4x blade žiletkový server do výše uvedeného šasi. Identická konfigurace

**Hardwarová specifikace**

- Server musí splňovat následující požadavky:

  - provedení žiletkové do výše popsaného šasi

- vpředu 2 pozice pro vložení disků 2,5 palců v rámečku s rozhraním SAS/SATA 12Gb a možností výměny za chodu
- rozhraní minimálně 2x USB 3.x (minimálně 1x USB uvnitř žiletky)
- možnost osazení 1 nebo 2 procesory nejnovější generace - dvě patice na CPU v jednom serveru (2x socket), podpora procesorů až s TDP 205W
- HW SAS řadič diskové kapacity s podporou RAID 1 a 5, 12Gb SAS
- podpora technologie zabezpečeného vzdáleného přístupu prostřednictvím datové sítě pro správu serveru před startem operačního systému
- bezagentová správa a monitoring serveru - bez nutnosti instalace agentů v OS
- management procesor s plně integrovanou grafickou konzolí s možností vzdálené správy
- minimálně osm v OS viditelných portů o celkové propustnosti alespoň 100GBit, z nich alespoň dva porty FC SAN s možností nastavení propustnosti v rozmezí 16 až 32 Gbit
- přenositelnost všech síťových identifikačních parametrů (MAC, WWN, SAN Boot apod.) mezi jednotlivými servery v rámci šasi nebo mezi více propojenými šasi v jednotném řídícím okruhu
- vysoce dostupné bezkabelové propojení FC
- vysoce dostupné bezkabelové propojení typu Ethernet/IP
- podpora technologie startu operačního systému z úložiště vzdáleného správce
- plná kompatibilita se serverovými systémy fakulty

- Požadované osazení serveru:
  - Minimální požadavky na CPU: 2x procesor s výkonem PassMark CPU Mark minimálně 15 000 (benchmark skóre určeno dle www.cpubenchmark.net, 3.2.2022) na procesor, s podporou HW virtualizace, DDR4 pamětí RAM, maximální spotřeba CPU (TDP) 130W na jedno celé CPU (všechna jádra)
  - Maximálně 8 fyzických jader na jedno CPU z důvodu optimalizace licenčních nákladů Microsoft Windows
  - každý server bude osazen minimálně 256 GB RAM DDR4 o frekvenci 2933 MHz s možností rozšíření minimálně na 0,75 TB RAM bez výměny již osazených RAM
  - v každém serveru 2x 2,5“ 240GB SATA SSD Read Intensive zabezpečený RAID1 pro boot operačního systému
  - Součástí dodávky jsou i kabelové redukce potřebné pro připojení standardního konektoru VGA (D-SUB 15) a USB (pokud jsou potřeba)

- Funkční specifikace
  - podpora vzdáleného přístupu k zařízení prostřednictvím vestavěného grafického rozhraní dohledu a plné konfigurace na bázi protokolu HTTPS

### 1.3 Server – rozhodovací

Určený pro provoz clusteru diskových polí níže, pro zajištění správy a rozhodovacího nodu clusteru diskových polí, 1ks rackového serveru umístěný v neutrální lokalitě mimo hlavní a sekundární serverovnu.

**Hardwarová specifikace rozhodovacího serveru**

- Server musí splňovat následující minimální požadavky:

  - server o velikosti 1U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely
  - dva CPU sockety v serveru
  - podpora persistentních paměťových modulů typu NVDIMM
  - podpora ochrany paměti Advanced ECC, Online spare, zrcadlení a FFT
  - možnost min. 8 pozic pro 2,5" hot-swap SAS/SATA/SSD disky
  - možnost rozšíření o min. 2 pozice pro 2x 2,5" hot-swap PCIe NVMe disky, nebo 4x hot-swap M.2 SSD moduly
  - disky musí mít rámečky vybaveny indikátorem varujícím proti vytažení disku na kterém se provádí datové operace, nebo musí být takový disk proti případnému nebezpečnému vytažení blokován
  - min. 5 portů USB 3.x, z toho minimálně 1x interní
  - 4x 1Gbit LAN porty s podporou Large Send and Receive offload capability, VLAN tagging, MSI-X, jumbo frames, IEEE 1588, VMware NetQueue a Microsoft VMQ nezabírající rozšiřující PCIe sloty
  - 2x 10Gbit LAN porty osazené optickými SR transceivery a s podporou VLAN

tagging, adaptive interrupt coalescing, MSI-X, NIC teaming (bonding), Tunnel offloads (NVGRE, VXLAN), TCP/Ip Stateless Offloads, Receive Side Scaling (RSS), jumbo frames a PXE boot.
    - 1x 1Gbit port pro management
    - větráky v serveru musí být vyměnitelné za provozu a redundatní
    - instalované napájecí zdroje musí podporovat řízení spotřeby CPU instalovaných v poptávaných serverech
    - napájecí zdroje splňující požadavky certifikace energetické účinnosti, např. ECOS Consulting 80 Plus (min. Platinum), případně dodavatel doloží, že jejich účinnost při napájení 230V je minimálně min. 94%

- Požadované osazení rozhodovacího serveru:
    - 2x procesorem s výkonem PassMark CPU Mark minimálně 15 000 (benchmark skóre určeno dle www.cpubenchmark.net, 3.2.2022) na procesor HT je požadován, L2 Cache min. 11 MB (pro všechna jádra, možné sdílení) s podporou HW virtualizace, DDR4 pamětí RAM, maximální spotřeba CPU (TDP) 130W na jedno celé CPU (všechna jádra) – identické procesory se servery v blade šasi v lokalitě 1 z důvodu snadné náhrady.
    - maximálně 8 fyzických jader na jedno CPU z důvodu optimalizace licenčních nákladů Microsoft Windows
    - operační paměť osazena minimálně 192GB RAM DDR4 o frekvenci 2933 MHz, osazená v optimální konfiguraci pro nabízený CPU, rozšiřitelná minimálně na 384GB RAM bez výměny již osazených RAM
    - osazeno min. 900GB čisté kapacity v RAID1 formou hot-swap 2,5" SSD vhodnými pro boot OS a provoz managementu virtuálních strojů, rozhodovacího nástroje pro disková pole a dalších nástrojů správy
    - 2x napájecí zdroj s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje min. 740W

**Požadavky na správu všech výše specifikovaných serverů**

- řízení přístupových práv k centrální části SW a k management nástrojům pomocí účtů Active Directory domény, autentizace uživatele PINem a certifikátem
- virtuální KVM (tj. převzetí textové i grafické konsole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače), včetně možnosti sdílení až čtyřmi uživateli současně u plně grafické konsole
- zapnutí, vypnutí a restart serveru na dálku
- namapování vzdálených medií Floppy/CD, image souborů a adresářů
- rozlišení grafické konzole 1600x1200 a vyšší
- možnost přesměrování terminálových služeb Windows na dedikovaný management port
- možnost využití běžných www prohlížečů integrovaných v desktopovém OS pro správu serverů (IE, Firefox)
- kódování Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) pro zabezpečení komunikace s běžnými www prohlížeči
- CLP a XML rozhraní pro skriptování
- podpora UEFI Secure Boot
- server musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného fimware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, musí být součástí nabídky.
- podpora detekce otevření chassis serveru
- musí umožňovat stabilizaci nežádoucích fluktulací frekvence procesoru mezi nativní a Turbo frekvencí
- musí umožňovat optimalizaci výkonu serveru v závislosti na zvoleném druhu zátěže
- volitelná komunikace přes dedikovaný management port
- možnost nastavit sdílenou komunikaci pro správu celého systému přes standardní integrovaný Ethernet port s možností využití technologie VPN
- možnost vyvolat NMI přerušení nedostupného OS
- možnost zasílání proaktivních hlášení o možných chybách v systému pomocí SNMP a také na uživatelsky definovanou emailovou adresu
- performance monitoring komponent (CPU, RAM, HDD, LAN) pro Windows a Linux OS, který umožní online i offline analýzu serverů

- měření a řízení spotřeby serveru s možností uzamknutí příkonu
- monitorování okamžité teploty a záznam hodnot do lokální db
- možnost skupinové správy rackových serverů prostřednictvím jedné servisní konzole
- možnost skupinového update firmware rackových serverů
- správa serverů umožňuje vzdálené monitorování a reporting událostí/závad i mimo firemní síť/VPN, v rámci globálního internetového portálu nebo cloud služby s podporou pro mobilní zařízení (Android, iOS)
- integrace správy žiletkového šasi s nástroji správy SAN infrastruktury a diskových polí pro jednotnou konzoli s možností ovládání a mapování všech HW prostředků
- v případě, že se jedná o licencované vlastnosti, je vyžadována možnost hromadné aktivace licencí všech poptávaných serverů
- licence pro integraci managementu HW serveru do konzole Hypervizoru (MSSC, vCenter)

- **Záruka na šasi a všechny výše uvedené servery**
  - rozšířená záruka a podpora výrobce serverů a šasi po dobu 5let, minimálně 24 x 7, 4h response time. Tato záruka musí být garantována přímo výrobcem.
  - technická podpora výrobce po dobu 60 měsíců v režimu 24x7 - software aktualizace (nové verze programového vybavení)

## 2) Storage SAN infrastruktura

Všechny nabízené prvky SAN infrastruktury do lokalit musí být stejného typu a výrobce, spravovatelné stejným způsobem a rozhraním, s kompatibilní správou. Prvky musí být propojitelné se stávající FC SAN infrastrukturou, která zůstane zachována (FC switch Brocade 8-16Gb viz Popis současného stavu) - na nativní úrovni, bez potřeby speciálních tzv. „kompatibilních“ módů.

Celá SAN infrastruktura musí být spravovatelná jedním společným nástrojem, určeným pro komplexní správu a provisioning blade serverů (virtualizace WWN a MAC adres, vytváření, správa a přiřazování serverových profilů s nastavením a BIOS/FW apod.), SAN infrastruktury (zejména nastavení SAN a zónování) a diskových polí (včetně vytváření a provisioningu volumů novým blade serverům nebo vytváření a provisioningu dalších volumů těmto serverům). Pokud takový nástroj nenabízí výrobce, uchazeč se zavazuje ho dodat/vyvinout jako součást celé dodávky tak, aby mohl být použit při prvotním nastavení a správě nově instalovaného prostředí. Cílem je získat jednotně a jednoduše spravovatelnou IT infrastrukturu, integrovanou do jednotného management rozhraní.

**Hardwarová specifikace SAN přepínačů**

Primární a sekundární lokalitu požadujeme osadit vždy párem identických přepínačů (celkem 4ks FC přepínačů) specifikovaných níže.

- SAN přepínače musí splňovat následující minimální požadavky:
  - SAN Přepínač Fibre Channel s podporou minimálně 8-16-32Gb rychlostí
  - minimálně 16 funkčních, licencovaných FC portů na přepínač, s možností rozšíření na 24 FC portů s rychlostí až 32Gb
  - 16x 32Gb SFP28 shortwave pro připojení serverového blade šasi a diskového pole v každém přepínači
  - 2x 16Gb SFP+ longwave (do 10km) pro připojení vzdálených lokalit, v každém přepínači

**Funkční požadavky na SAN přepínače**

- společná správa a integrace zónování přepínačů v rámci správy blade šasi
- web management
- REST API pro podporu integrace do management nástrojů
- podpora propojení mezi přepínači na vzdálenosti do cca 10km

**Fibre Channel kabeláž pro připojení SAN přepínačů k serverovým a úložným zdrojům**

- 60x FibreChannel multimode kabel OM4 v délce 5 metrů, zakončený LC konektory
- 10x FibreChannel multimode kabel v délce 15 metrů, zakončený LC konektory
- 10x FibreChannel singlemode kabel v délce 15 metrů, zakončený LC konektorem a E2000 konektorem na druhé straně

**Záruka a služby pro Fibre Channel SAN přepínače**

- rozšířená záruka a podpora výrobce/dodavatele přepínačů po dobu 5let, minimálně 24 x 7, 4h response time. Tato záruka musí být garantována přímo výrobcem.
- technická podpora výrobce po dobu 60 měsíců v režimu 24x7 - software aktualizace (nové verze programového vybavení)
- služba instalace a implementace SAN infrastruktury včetně propojení se stávající SAN (16Gb Brocade/Broadcom v sekundární lokalitě)

## 3) Centrální disková úložiště

V cílovém stavu zadavatel vyžaduje robustní infrastrukturu odolnou vůči pádu jedné nebo druhé lokality tak, aby zbývající lokalita byla schopna převzít provoz aplikací z havarované lokality v rámci jednotek minut. Nutnou podmínkou dosažení takového provozního stavu je provádění replikace dat mezi diskovými úložišti v reálném čase. V rámci efektivního využití stávajících investic požadujeme dodávku nového pole do primární serverovny, kompatibilního na management úrovni a replikační úrovni se stávajícím polem HPE 3Par 8200, které bude umístěno v sekundární serverovně. Dále požadujeme rozšíření kapacity stávajícího diskového pole HPE 3Par 8200 na kapacitu a výkon definované níže v kapitole „Rozšíření stávajícího diskové pole HPE 3Par 8200“. Cílem je vytvoření synchronních replikačních vztahů mezi novým a stávajícím polem a jejich clustering do společného automatizovaného řešení, spravovaného z jedné konzole spolu s blade šasi a serverovou infrastrukturou.

V případě, že navržené diskové pole není 100% kompatibilní pro replikační činnost se stávajícím diskovým polem HPE 3Par 8200, uchazeč může replikaci vyřešit jiným vhodným způsobem při zachování:

- ochrany investice do stávajícího pole HPE 3Par 8200 rozšířením jeho kapacity a výkonu na níže požadované hodnoty v kapitole „Rozšíření stávajícího diskové pole HPE 3Par 8200“
- společné správy serverové, SAN a storage infrastruktury z jednotného rozhraní
- zajištění virtualizační a/nebo replikační mezivrstvy mezi diskovými poli a její začlenění do nástroje společné správy (tak, aby například nebránila požadovanému automatickému provisioningu kapacity prostředky centrálního nástroje správy serverové infrastruktury)
- zajištění synchronní repliky s clusterem diskových kapacit v novém poli a stávajícím poli, s automatickým překlopením provozu v případě výpadku primární serverovny

### 3.1 Diskové pole

Nové diskové pole pro umístění do primární serverovny, vhodné pro enterprise provoz 24x7, s nízkou latencí pro provoz zejména virtuální infrastruktury. Součástí dodávky musí být jedno diskové pole s blokovým přístupem, minimálně v následující konfiguraci a s následujícími vlastnostmi (výrazy jako „podpora“, „možnost“ a podobně jednoznačně znamenají, že dané funkce a vlastnosti musí být součástí dodaných funkcí a vlastností diskového pole či infrastruktury tak, aby je mohl provozovatel použít bez dalších nároků například na licence či další software):

- Diskové pole musí splňovat následující minimální požadavky:
  - all flash konfigurace bez použití rotačních médií, s možností je v budoucnu instalovat (podpora hybridní konfigurace)
  - max 2RU (rackunits) výšky, instalace do racku (rack není součástí poptávky)
  - jednofázové napájení, plně redundantní. Diskové pole nesmí mít žádný single point of failure.
  - dva plnohodnotné řadiče, schopné plně zastoupit provoz v okamžiku havárie řadiče, cache paměti v něm a podobně. Řadiče diskového pole musí být zdvojené a na sobě nezávislé, vzájemně propojené pomocí pevného spoje (backplane v šasi). Architekturu pole, složeného z jednotlivých nodů propojených kabely či přepínači, neakceptujeme z důvodu bezpečnosti a spolehlivosti. Oba řadiče v plně active/active konfiguraci, se zcela rovnocenným přístupem k jakémukoli flash disku v diskovém poli a s rovnocenným přístupem ze strany serverů (round-robin MPIO).
  - možnost budoucího rozšíření pole o rotační disky v počtu minimálně 8ks. Volné sloty na

rotační disky požadujeme v rámci této dodávky.

- neomezená podpora běžných operačních systémů (Windows, Linux, VMWare, HyperV, apod.) bez omezení počtu připojených serverů
- ochrana dat v cache v řadiči při výpadku napájení po neomezenou dobu
- FibreChannel 32Gb, minimálně 4 porty na řadič (8 na diskové pole)
- Ethernet porty pro možnost záložní cesty replikace po IP na druhé diskové pole, 10Gb, minimálně 2 porty na pole (1 na řadič), replikační funkce je nutnou součástí této nabídky
- oddělený port na management a správu diskového pole. Všechny dostupné funkce diskového pole a jeho správy budou součástí řešení v neomezené kapacitě, neomezeném počtu připojených serverů apod.
- cache paměť o velikosti minimálně 256GB na pole bez uvažování rozšíření cache s pomocí SSD nebo NVMe disků
- podpora virtualizovaných RAID režimů, zejména RAID6
- možnost instalace NVMe disků, SSD SAS disků a rotačních SAS disků 10k otáček
- čistá kapacita (bez uvažování redukčních algoritmů) s využitím RAID6 minimálně 56 TiB na SSD/allflash vrstvě. Kapacita musí být výkonově vhodná k použití pro virtualizované servery a produkční systémy, dle doporučení výrobce.
- Kapacita jednoho SSD média nesmí být vyšší než 8TB.
- minimálně 12 využitých datových médií k dosažení požadovaného výkonu. V rámci nabídky účastník doloží deklarovaný výkon 60.000 IOps pro 16kB random IO, poměr čtení/zápis 60/40, max response time 1ms při uvažování maximálního cache hit poměru 20%. Tento požadavek zahrnuje zapnuté veškeré datové redukční funkce (ThP, komprese, deduplikace) na celé kapacitě diskového pole. Doložení výstupem ze sizing nástroje je dostatečné. Zadavatel si vyhrazuje právo výkon navrženého diskového pole před akceptací dodávky otestovat. Pokud při zapnutých redukčních funkcích (minimálně komprese a deduplikace) nebude výkonu dosaženo (na datovém vzorku se zaplněním minimálně 80% kapacity pole, s testovací oblastí přes celý datový vzorek), bude pole považováno za nevyhovující. V takovém případě se dodavatel na vlastní náklady zavazuje bezodkladně výkon pole navýšit tak, aby bylo výkonu dosaženo.
- distribuovaný hot spare prostor pro okamžité obnovení dat z kapacity vadného disku. Sparing funkce pro urychlení procesu by rovněž měla rekonstruovat pouze fyzicky zapsaná data na disku, nikoli prázdný diskový prostor.
- podpora redukčních funkcí minimálně na úrovni komprese a deduplikace. Schopnost výkonově obsloužit 100% kapacity pole se zapnutými redukčními funkcemi.
- možnost redukční funkce zapnout/vypnout na úrovni jednotlivého volume
- podpora tenkého provisioningu a alokace a dealokace kapacity podle aktuálních uložených dat, včetně integrace s dealokačními funkcemi VMWare ESXi.
- možnost vytváření „tenkých kopií“, nebo snapshotů ze všech typů výše uvedených volumů bez omezení. Možnost vytvoření minimálně 120 snapshotů z každého volumu a možnost časového plánování s častým cyklem (cca 5-10minut)
- software a integrace funkce snapshotů s aplikacemi pro synchronizaci vytváření těchto kopií dat v konzistentním stavu, pro nejběžnější typy aplikací (zejména pro MS SQL, VMWare, Oracle)
- replikace (synchronní i asynchronní) na stávající diskové pole, podpora vytvoření clusteru diskových polí se stávajícím polem tak, aby při výpadku jednoho diskového pole druhé pole okamžitě a bez výpadku provozované aplikace převzalo funkci havarovaného pole či celé lokality. Takový cluster musí být chráněn proti poškození a případným split-brain situacím alespoň pomocí tzv. witness nodu majoritou funkčních členů clusteru. Předpokládáme umístění rozhodného nodu clusteru ve formě softwareového balíčku na výše uvedený rozhodovací server.
- Pokud navržené diskové pole není kompatibilní s replikačními funkcemi stávajícího diskového pole HPE 3Par 8200, či jej není možno s tímto polem clusterovat, dodavatel může replikaci vyřešit jiným vhodným způsobem (viz úvod kapitoly Disková pole).
- podpora nastavení QoS – Quality of Service – omezení výkonu jednotlivých volumů či skupiny volumů alespoň na úrovni MBps, IOPs, nastavení cílové latence pro danou aplikaci či serverovou skupinu
- software pro zálohování dat formou snapshotů s možností napojení na veřejné cloudové služby. Nabídka kapacity veřejného cloudového úložiště není součástí aktuální poptávky, diskové pole však takovou replikaci musí umožňovat.
- automatické hlášení poruch a chybových či podezřelých stavů do dohledového centra výrobce
- autonomní správa a hlídání dodržování best practices s možností hluboké analýzy používání s doporučeními na úpravu, zahrnující jak diskové pole, tak infrastrukturu a virtualizaci (minimálně pro diskové pole, servery, HyperV a VMWare v jednom společném grafickém rozhraní) – s možností vizualizace zatížení VM, hypervisoru HyperV a VMWare, CPU, RAM, disků a volumů, s vizualizací vzájemného ovlivňování zdrojů a

virtuálních strojů, volumů, s doporučeními na úpravu konfigurace. Monitoring s identifikací nejaktivnějších virtuálních strojů, nejvyšších latencí, nejzatíženějších volumů apod.

- **Záruka**
  - rozšířená záruka a podpora výrobce diskového pole po dobu 5let, minimálně 24 x 7, 4h response time. Tato záruka musí být garantována přímo výrobcem diskového pole.
  - v rámci rozšířené podpory se výrobce a dodavatel zavazují, že během podpory vymění bez dodatečných nákladů jakékoli poškozené či vypsané flashové médium, bez omezení počtu zápisů.

### 3.2 Rozšíření stávajícího diskové pole HPE 3Par 8200

Jedná se o již pořízené a zadavatelem provozované diskové pole a to v konfiguraci 8x1.92TB SSD, 10TiB čisté kapacity allflash, s FC připojením.

Zadavatel požaduje rozšíření kapacity tohoto diskového pole a zajištění repliky z nově dodávaného pole dle kapitoly 3.1. Pro zajištění tohoto požadavku se dodavatel zavazuje dodat v rámci projektu systém jednotné správy, monitoringu a provisioningu stávajících komponent storage infrastruktury a infrastruktury dodávané.

Součástí nabídky a dodávky musí být pro toto diskové pole:

- rozšíření allflash diskové kapacity pole na minimálně 46TiB čisté využitelné kapacity v RAID6, bez uvažování jakýchkoli redukčních technik (komprese, deduplikace apod.)
- rozšíření musí být realizované SSD disky s maximální kapacitou 4TB
- rekonfigurace stávající kapacity tak, aby byla bezvýpadkově zahrnuta do celkové kapacity pole
- vybavení pole licencí pro zajištění repliky a clusteru s nově dodávaným polem (viz kapitola 2.1 Diskové pole pro primární serverovnu)
- vybavení pole minimálně 4x FC port 16Gb pro replikační interface
- zajištění a konfigurace replikace a clusteru diskových polí viz 3.1 Diskové pole pro primární serverovnu. Pokud navržené diskové pole do primární serverovny není kompatibilní s replikačními funkcemi stávajícího diskového pole HPE 3Par 8200, či jej není možno s tímto polem clusterovat, dodavatel může replikaci vyřešit jiným vhodným způsobem - viz úvod kapitoly Disková pole.

- **Záruka**
  - rozšířená záruka a podpora výrobce diskového pole (zahrnující stávající kapacitu, řadiče a funkce diskového pole i kapacitu v rámci rozšíření) po dobu 5let, minimálně 24 x 7, 4h response time. Tato záruka musí být garantována přímo výrobcem diskového pole.
  - v rámci rozšířené podpory se výrobce a dodavatel zavazují, že během podpory vymění bez dodatečných nákladů jakékoli poškozené či vypsané flashové médium, bez omezení počtu zápisů.

### 3.3 Pásková knihovna

Pro účely zajištění zálohování a archivace dat celé infrastruktury zadavatel požaduje páskovou knihovnu s předpokládaným umístěním do primární serverovny a s minimálně následujícími parametry:

- pásková knihovna LTO8 s rozhraním Fibre Channel minimálně 8Gb
- 2x LTO8 pásková mechanika, minimálně 24 slotů na pásky, všechny sloty budou osazené LTO8 ReadWrite médiem
- software pro identifikaci chyb při čtení a zápisu, monitoring provozu páskové knihovny a mechanik, sledování zátěže jednotlivých mechanik a využití médií s jednoduchým grafickým rozhraním
- rackmount provedení, maximální výška 2RU
- web based rozhraní pro vzdálenou správu páskové knihovny, kontrolu osazení slotů páskami apod.
- podpora čtení čárových kódů na páskových médiích
- 1x čistící médium
- rozšířená podpora výrobce páskové knihovny po dobu 5 let, 24x7x4h response

- instalace a základní implementace páskové knihovny do SAN infrastruktury

- **Záruka**
  - rozšířená záruka a podpora výrobce diskového pole po dobu 5let, minimálně 24 x 7, 4h response time. Tato záruka musí být garantována výrobcem páskové knihovny.

## 4) Základní programové vybavení

**Specifikace základního programového vybavení** (software)

 **Operační systém** musí splňovat následující požadavky:
  - plně kompatibilní se stávajícím systémem Zadavatele
  - časově neomezená akademická licence v poslední verzi vydané výrobcem k datu dodání s bezplatnou aktualizací na všechny nové verze po dobu minimálně 3 let od výročí příslušné smlouvy zadavatele, a to je od 1. 9. 2020

 **Soubor software na pro běh virtualizovaných aplikačních serverů**, jejich řízení a dohled musí splňovat následující požadavky:
  - systém s hypervizorem musí umožňovat běh stávajících aplikačních serverů a jejich volný přesun mezi stávajícími servery fakulty i těmito novými
  - nadstavba musí umožňovat interaktivní i automatizované řízení využití dostupných zdrojů výkonu i kapacity všech částí systému zahrnutého do správy, dynamicky optimalizovat virtualizované prostředky k zajišťování vysoké dostupnosti, umožňovat správu aplikací založenou na službách i ucelený dohled nad jednotlivými součástmi systému i aplikacemi
  - systém musí poskytovat škálovatelnost, flexibilní úložiště, vysokou dostupnost, efektivní správu a možnost propojení s cloudovými službami
  - počet běžících, řízených a dohledovaných aplikačních serverů (pro fyzický server se dvěma procesory) není kromě výkonnosti HW nijak omezen ani technicky ani licenčně. Tato licence pro operační systém pro neomezený počet virtualizovaných instancí je kompatibilní se stávajícími licencemi zadavatele.

## 5) Ochrana perimetru

Nové řešení bude funkčně nahrazovat a rozšiřovat stávající zastaralé a nevyhovující řešení. Koncepčně předpokládáme náhradu za plnohodnotné nové řešení se dvěma nody firewallů v provedení HW appliance (dále jen FW) s plnou redundací dále popsanou. Za účelem maximální redundance a odolnosti proti výpadkům zadavatel požaduje lokalitní rozdělení FW a to do primární a sekundární serverovny po jednom kusu do každé. Pro vzájemné propojení FW k zjištění vysoké dostupnosti (dále jen HA) budou k dispozici dvě vyhrazená optická dvouvlákna Single mode s konektorem E2000 vedené mezi serverovnami. Pro případ výpadku této dedikované HA linky bude firewall umožňovat zálohu HA pomocí datové komunikaci vedené přes páteřní switche metalickým min. 1Gbit portem např. pomocí vyhrazené VLAN nebo jiným vhodným způsobem.

Základní (intranetové) připojení na síťovou LAN infrastrukturu zadavatele bude realizováno optickým propojením mezi každým jedním FW (a centrálním(i) switch(y) (primární serverovna - HPE JL624A - Aruba 8320 a sekundární serverovna - Alcatel OS-7700) a to rychlostí min.10Gbit pro každou jednu serverovnu. Dále je požadována možnost řešit oddělení segmentů DMZ, studentské nebo přístrojové sítě virtuálně nebo pomocí fyzických tras. Nejvhodnější topologické řešení bude zvoleno v rámci implementace.

Nové řešení nadále předpokládá WAN připojení na stávající topologii dvou redundantních optických linek pro připojení k internetu (metropolitní síť CESNET) o kapacitě 10Gbit každá s tím, že hlavní linka bude vedená přímo do primární serverovny a záložní linka do serverovny sekundární. Pomocí páteřních switchů a VLAN bude zajištěno, aby každý z FW měl k dispozici na svých portech jak

hlavní, tak záložní linku do internetu. Pro dosažení maximální kapacity propojení mezi daným FW a páteřním switchem je možné využít/sdružit oba 10Gbit optické porty na FW.

Přepínání nedostupné linky bude nadále zajištěno pomocí funkcinality BGP protokolu. Toto řešení je již plně funkční v rámci stávajícího řešení FW a je tedy možné ho přenést v plném rozsahu i na nové řešení.

Správa vlastních politik, ukládání událostí a reporting by měl být od vlastních hardwarových FW oddělen. Zadavatel umožní instalaci a provoz management software ve virtuálním prostředí (Microsoft Hyper-V) na virtuálním serveru k tomu určeném (virtuální server není předmětem dodávky). Řešení musí být koncipované tak, že (ne)dostupnost management software a serveru nesmí omezovat vlastní funkci firewalu, tj. plná funkcionalita FW je na managementu serveru provozně nezávislá.

*Pozn.: výše uvedený popis je pouze základním nutným požadavkem na síťovou topologii pro připojení FW s ohledem na maximální využití kapacity internetových linek a též s ohledem na vysokou odolnost cílového řešení proti chybám a výpadkům. Konkrétní konfiguraci nad rámec výše stanoveného dohodne zadavatel s uchazečem v rámci instalace a konfigurace FW s ohledem na konkrétní technické možnosti a s ohledem na „nejlepší provozní praxi" nabízeného řešení FW .*

Firewall musí mít zabudovanou IPS technologii a poskytovat ochranu před novými typy útoků. Krom antivirových ochran by měly umět pracovat s technologií, která dokáže určit, zdali se ve stahovaných souborech nemůže objevit riziková aktivita při běžném prohlížení uživatelem.

**Základní požadavky**

- Firewallové řešení by mělo být koncipováno jako komplexní UTM (Unified threat management). Toto řešení v sobě integruje kromě samotného firewallu i antivirovou ochranu, systém pro detekci/prevenci průniků a filtrování obsahu webové komunikace. UTM firewall umožňuje filtrování na úrovni 3. a 7. vrstvy modelu OSI.
- Nově navržené firewally musí v HA konfiguraci podporovat variantu Active/Active a řízené pomocí min jedné hlavní dedikované optické linkou a min. jedné záložní linky realizované např. pomocí metalických portů a switchů zadavatele
- Musí zachovat minimálně současnou úroveň zabezpečení a přidat nové prvky reagující na aktuální bezpečnostní hrozby zejména IPS funkcionalitu a ochranu Zero-Day a neznámými útoky. Umožní také kontrolu šifrovaného připojení.
- Musí umožňovat bezpečné připojení z prostředí internetu do intranetu (VPN, přístup na RDP, vzdálený management vybraných služeb v intranetu) a sofistikovaný a bezpečný přístup do/z DMZ.
- Správa pravidel a politik nastavení prostřednictvím grafického těžkého nebo plnohodnotného grafického lehkého webového klienta a možnost správy přes scriptové řádkové rozhraní
- Navržené řešení musí obsahovat bezpečnostní řešení (firewally) od výrobce, jehož produkty procházejí pravidelným testováním a kontrolou ze strany auditorské společnosti Gartner nebo obdobné.

**Technické specifikace**

- <u>Řešení musí splňovat následující minimální HW požadavky:</u>

  - Řešení pomocí HW fyzického zařízení (HW appliance) certifikovaného výrobcem, dva nezávislé boxy pro zajištění HA
  - Fyzická síťová rozhraní - jednotlivé porty musí být použitelné pro připojení jakéhokoli typu síťového provozu - LAN, WAN, DMZ, připojení externího subjektu
  - Počet fyzických síťových rozhraní minimálně 2 x 10GBit SFP+ slotů včetně SM SFP+ modulu, 10 x 1GBit ethernetových rozhraní, 8 x SFP slot).
  - Minimální velikost interní diskové kapacity 240 GB (doporučeno 100 GB a více) bez pohyblivých částí (SSD), pro dočasné ukládání logů v případě nedostupnosti management serveru.
  - provedení umožňující montáž do racku 19 palců s výškou maximálně 1U a maximálně hloubkou 80 cm. Pokud tato montáž není standardní možností,

dodávka musí obsahovat montážní kit pro instalaci do 19" datového rozvaděče.
    - 2 pozice pro moduly napájecích zdrojů vzadu
    - podpora redundance napájecích zdrojů s možností výměny za běhu (hot swap)
    - pokročilá podpora vrstvy 2 a 3 datového modelu ISO
    - vestavěné rozhraní pro management interface s podporou ethernet RJ45 min. 10/100Mbit/s
    - chlazení s redundancí (směr chladícího vzduchu od čelního panelu k zadnímu)
    - napájení 230 V 50 Hz se samostatným přívodem pro každý napájecí modul
    - soulad se všemi požadavky příslušných platných norem (bezpečnost, EMC, apod.)

  Požadované osazení FW:
    - 2 moduly zdrojů s redundancí 1+1

  Požadované příslušenství (v počtu dle přílohy č. 1 ZD - položkový rozpočet)
    - Optické SFP transceivery Single mode pro zajistění HA + příslušná optická propojovací kabeláž
    - Optické SFP+ transceivery MM pro zajištění primárního 10Gbit propojení hlavní a záložní WAN linky do obou FW a obou páteřních switchů. Transceivery musí být s daným páteřním switchem plně kompatibilní + příslušná propojovací optická kabeláž
    - Optické SFP transceiverymoduly MM s rychlostí min 1Gbit pro fyzické propojení min. DMZ a studentská síť + příslušná propojovací optická kabeláž
- Z důvodu zachovaní kompatibility a zachování pravidel hospodářské soutěže mohou být požadované transceivery OEM Jejich plnou kompatibilitu a bezproblémové fungování v infrastruktuře zadavatele i v nabízeném řešení FW garantuje uchazeč.
- LTE modem plně kompatibilní s FW pro umožnění nezávislého přístupu do managementu FW.

**pozn: Pokud navržené řešení vyžaduje s ohledem na jeho technologickou koncepci osazení jinými/dalšími moduly nebo jinou kabeláž nad rámec uvedené, nacení je účastník do přílohy položkový rozpočet jako součást položky NG Firewall a uvede do samostatné přílohy s popisem a označením.*

- <u>Řešení musí splňovat následující funkční požadavky:</u>

    - Propustnost FW brány během operace Stateful Packet Inspection s UDP pakety o velikosti 1518B je minimálně 35Gbps. Během stejné operace, při zpracování malých UDP paketů o velikost 64B, nesmí minimální propustnost FW brány klesnout pod 50% udané maximální hodnoty.
    - Propustnost IDS/IPS systému minimálně 10 Gbps.
    - Možnost blokování hrozeb včetně síťového provozu přenášeného šifrovaným připojením SSL (vč. TLS 1.3), propustnost kontroly SSL minimálně 8 Gbps.
    - Podpora protokolu IPv4 a IPv6 v totožném funkcionality
    - Podpora agregace portů (802.3ad - zvýšení propustnosti propojovací linky) spolu s technologii 802.1q.
    - Minimální počet podporovaných VLAN = 1024.
    - Podpora Active-Active (A-A), Active-Passive (A-P) clusteru, se stavovou synchronizací, požadována dodávka a implementace HA řešení v režimu Active/Active jako lokalitní cluster.
    - Stavová synchronizace TCP, UDP a NAT spojení.
    - Autentizace uživatelů min. podpora Microsoft Active Directory (LDAP), RADIUS, TACACS.
    - Podpora dynamického routování min. BGP, OSPF, OSPFv3 a RIP.
    - Podpora řízení kvality linky pomocí QOS
    - Implementovaný systém ochrany proti síťovým útokům – systém IDS/IPS.
    - Detekce a řízení síťových aplikací. Databáze aplikací musí obsahovat minimální počet rozpoznávaných aplikací 3000
    - Ochrana proti aktivitě botnetů - reputace IP adres, DNS a URL záznamů
    - Blokování komunikace na IP adresy řídících center botnetů. Detekce aktivit botnetů pomocí behavior analýzy
    - Prevence zero-day utoků na základě typu a obsahu komunikace.
    - Možnost rozšíření o řešení pro emulaci hrozeb ve virtuálním sandbox prostředí. Podporované typy emulovaných souborů: exe, pdf, archivy.
    - Filtrace webových stránek dle kategorií a uživatelských identit.
    - Ochrana proti virům, spamu a malware.
    - Konfigurace bezpečnostní politiky prostřednictvím GUI rozhraní. Vzdálené

připojení pomocí protokolů SSH a HTTPS.
- Podpora debuggování problémových scénářů na úrovni L2 - L7.
- Podpora pravidelného automatického zálohováni konfigurace (na základě časového rozvrhu), s možností automatického (zabezpečeného) nahrání na vzdálený server.
- Podporovaná možnost ukládat bezpečnostní logy na fyzicky oddělenou management platformu (centrální management).
- Podpora dvoufaktorové autentifikace pro VPN klienty (např. ověření AD + token, možnost využití machine/user certifikátu v PC).
- Monitoring firewallů, reporting provozu až na ověřeného uživatele atd. (SW pro monitoring a reporting bude podporovaný pro provoz ve virtuální platformě Microsoft Hyper-V).
- Licence a výkon minimálně 1500 aktivních, současně pracujících uživatelů.

- Detailní specifikace funkčních požadavků **na Firewall**

Next-generation firewall musí zvládat detekovat nové bezpečnostní hrozby, mezi které patří cílené i obecně zaměřené útoky na aplikace typu klient/server a jejich data. Tyto útoky se rozlišují i na aplikační vrstvě a mohou zahrnovat sofistikované pokusy o narušení v rámci protokolů a metod přístupu k datům jako je HTTP, XML, XSS, přetečení bufferu nebo SQL injection. Firewall musí být schopen detekovat jednotlivé typy aplikací a posuzovat, jestli datový tok v těchto aplikacích nevykazuje nějaké anomálie, které by mohly být součástí nějakého útoku.

Firewall musí být schopen definovat jednotlivá pravidla, ideálně na objektové úrovni. Musí být schopen ve svých politikách používat odkazy na jednotlivé aplikace nejen definované pomocí TCP a UDP portů, ale hlavně rozlišovat aplikace například zapouzdřené v http provozu (např. Skype, MS Teams, Teamviewer, torrenty atd.).

V pravidlech musí umožňovat použití uživatelských skupin definovaných v MS Active Directory. Musí být schopen jednotlivá pravidla omezovat na časové úseky, měl by mít možnost pravidla dočasně deaktivovat.

- Licenčně neomezený počet pravidel (filter, nat a další)
- Povolování jednotlivých toků.
- Tvoření pravidel s použitím identit uživatelů a počítačů v MS AD doméně.
- Vynucení si autentizace před povolením toku v rámci jednotlivých pravidel.
- Překlad adres s plnou stavovou kontrolou mezi jednotlivými porty firewallu.

- Detailní specifikace funkčních požadavků **WEB Security**

Je požadováno jednotné zabezpečení webové komunikace, včetně detekce konkrétních webových aplikací v http a https provozu.

Web security funkcionalita umožní omezovat pásmo pro použití jednotlivých pravidel (aplikací) a bude umožňovat i časové rámce na povolování jednotlivých kategorií.

Reportovací nástroje musí umožnit vytvořit přehledné a jednoduše přehledy o jednotlivých uživatelích a jeho aktivitách v síťovém provozu procházejícím firewallem. Filtrace minimálně na rovni uživatel/datumové a časové rozmezí/typ komunikace (aplikace, protokol, port, apod). Logování veškerého síťového provozu je nutnou podmínkou.

Sledování a vyhodnocování aktivity je možná na bázi jeho AD autentizace. Pravidla bude možné vytvářet na bázi uživatelů a/nebo jejich předdefinovaných skupin. Kromě blokování uživatelů, vybraných zdrojů a služeb bude též možné podle obsahu a podle kategorií. Řešení zajistí skenování obsahu a souborů v rámci komunikace.

- Detailní specifikace funkčních požadavků **EMAIL Security**

Navržené firewally musí poskytnout anti-spam ochranu, včetně kontroly obsahu a posouzení reputace IP adres a prověření antivirem.

- Detailní specifikace funkčních požadavků **INTRUSION DETECTION/PREVENTION SYSTEM**

IPS (systémy pro detekci a prevenci průniku) v navržených firewallech musí mít následující funkce minimálně:

- identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, následném blokování této činnosti a také její nahlašování.
- IPS s detekcí založenou na signaturách, ale i na anomáliích v síťovém provozu.
- Zároveň s detekcí konkrétních typů aplikací je možné dále zvyšovat efektivitu IPS systému – učící se systém
- Pro active/active topologii je důležité, aby IPS fungovalo jako distribuovaný systém.
- Vytváření a aplikace různých politik IPS systému.

- Detailní specifikace funkčních požadavků **Vzdálený přístup (VPN)**

Firewall musí poskytovat VPN jako bezpečné a jednoduché řešení pro připojení k podnikovým aplikacím přes internet ze smartphonu, tabletu nebo počítače. Nové řešení musí poskytovat komplexní vzdálený přístup na vrstvě Layer-3 VPN i SSL VPN. Je požadováno, aby VPN klient uměl komunikovat i za pomocí WEB SSL (443) portů, z důvodu možných omezení na straně poskytovatele internetového připojení.

VPN musí splňovat následující požadavky:

- SW licence pro neomezený počet přistupujících VPN uživatelů.
- Bezpečné připojení pro chytré telefony, tablety, počítače a notebooky.
- Poskytovat klient-based a Web-based připojení VPN.
- Snadný přístup pro mobilní pracovníky využívajících zařízení pod správou administrátorů ale i bez ní.
- Bezpečnou komunikaci s osvědčenou šifrovací technologií.
- Ověření oprávněných uživatelů s dvoufaktorovou autentizací, ale i párování typu uživatel-zařízení.
- Jednotné řízení pro jednoduché nasazení a správu.
- Použití uživatelských certifikátů.

- Detailní specifikace funkčních požadavků **na Management**

Zařízení musí poskytovat plnohodnotný lokální management pomocí web GUI a SSH CLI.

U zařízení musí být možnost kombinace lokálního a centrálního managementu (např. v době výpadku management serveru nebo konektivity k němu, včetně možnosti později importovat lokálně provedenou konfiguraci do centrálního management serveru).

Centrální management, logování a reporting nástroje musí splňovat:

- Možnost fyzicky oddělit management od firewall platformy - na samostatném hardware / virtuálním Hyper-V serveru. V rámci implementace bude požadován nezávislý management na virtuálním Hyper-V serveru.
- Podpora různých profilů administračních účtů, možnost definice úrovně přístupů na různé management komponenty s privilegiem: čtení / zápis a čtení / žádná práva.
- Podpora tvorby revizí jednotlivých verzí bezpečnostní politiky.
- Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů.
- Management musí být schopen dohledat pro každý objekt, jeho výskyt v aktivních i neaktivních pravidlech, nebo jiných objektech (např. ve skupinách)
- Možnost segmentace politik do samostatných logických oddílů.
- Musí umožňovat vkládání a definici uživatelských notifikací v případě, že se klient chová v rozporu s bezpečnostní politikou.
- Musí umožnit konfiguraci detekce anomálního chování sítě (detekce spammerů, aktivity botnetů, reputace koncových stanic).

- Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky
- Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálném čase minimálně (využití paměti, CPU, počet navázaných spojení, propustnost).
- Centrální ukládaní logů z firewall platforem.
- Podpora práce s bezpečnostními logy a to zejména filtrace a prohledávaní logů, export do souboru, definování vlastních filtrů.
- Podpora pravidelného automatického zálohováni konfigurace (na základě časového rozvrhu), s možností nahrání zálohy na vzdálený server.
- Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log záznamů je 100GB.

- Analýza a korelace bezpečnostních událostí / logů:
  - Podpora korelace bezpečnostních logů a incidentů.
  - Výrobce musí poskytovat pravidelné updaty pro nové verze logů nabízeného firewall řešení
  - Musí graficky zobrazovat jednotlivé kategorie událostí ve formě interaktivních koláčových a časových grafů.
  - Musí implementovat vyhledávání zadané hodnoty skrze celou databázi událostí (bez nutnosti definice prohledávaných atributů).
  - Musí umožnit seskupovaní výsledků vyhledávaní dle jednotlivých atributů (typ incidentu, zdroje, uživatelského jména).
  - Musí umožnit definici a permanentního ukládání vlastních filtrů událostí pro jednotlivé uživatele.
  - Musí podporovat automatické reakce na definované bezpečnostní události – minimální akce: poslat email, SNMP trap do interního systému.

- **Záruka k dodávanému řešení**

  - minimálně 60 měsíců s garantovanou dobou opravy do konce následujícího pracovního dne od nahlášení), tato záruka musí být garantovaná přímo výrobcem zařízení
  - technická podpora výrobce po dobu 60 měsíců v režimu 24x7 vč. software aktualizace. Nové verze programového vybavení vč. trvale a pravidelně aktualizované datové základny pro aktualizaci všech bezpečnostních systémů (včetně AV, IPS, antispam a dalších signatur)