# Kupní smlouva

(dále jen „smlouva“)

dle § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku,  
ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

1. **Smluvní strany**
   1. **Kupující:**  **Město Šlapanice**

se sídlem: Masarykovo náměstí 100/7, 664 51 Šlapanice

zastoupen: Mgr. Michaela Trněná, starostka

Identifikační číslo:  00282651

DIČ: CZ00282651

(dále jen jako „**kupující**“)

* 1. **Prodávající:** ……………………………

se sídlem: ……………………………

zastoupen: ……………………………

zástupce ve věcech technických: ……………………………

IČ: ……………………………

Bankovní spojení: ……………………………

Telefon: ……………………………

E-mail: ……………………………

(dále jen jako „**prodávající**“)

Obě smluvní strany po vzájemném projednání a shodě uzavírají tuto smlouvu:

1. **Předmět smlouvy**
   1. Účelem této smlouvy je dodávka zařízení včetně jeho implementace a napojení na ostatní infrastrukturu kupujícího (včetně současně budované infrastruktury) a následné předání funkčního kompletu kupujícímu, zaškolení administrátorů, uživatelů, rozvoje a podpory. Zařízení je určené pro kupujícího (Město Šlapanice) a pro jeho organizace.
   2. Podkladem pro uzavření této smlouvy je nabídka prodávajícího, podaná v zadávacím řízení nazvaném **„V 00812 – Zvýšení kybernetické bezpečnosti pro infrastrukturu města Šlapanice“, část 2: Dodávka infrastruktury** (dále jen „Veřejná zakázka“), zadávaném dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.
   3. Touto smlouvou se prodávající zavazuje dodat za podmínek v ní sjednaných kupujícímu zboží, uvedené v článku 3. této smlouvy a převést na něj vlastnické právo k tomuto zboží.
   4. Kupující se zavazuje zboží převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu stanoveném touto smlouvou.
   5. Předmět plnění bude spolufinancován z dotačního projektu (dále jen „Projekt“) **„Zvýšení kybernetické bezpečnosti pro infrastrukturu města Šlapanice“, reg. č. CZ.31.2.0/0.0/0.0/23\_093/0008390**, financovaného z Národního plánu obnovy (dále jen „NPO“).

**3. Předmět koupě**

1. Předmětem smlouvy je dodávka **hardware vč. software a jeho implementace**, jehož specifikace včetně technických parametrů je uvedena v příloze č. 1 této smlouvy (dále jen „zboží“).
2. Součástí předmětu koupě jsou i veškeré doklady požadované právními předpisy k používání předmětu koupě - zboží. Prodávající prohlašuje, že předmět koupě splňuje veškeré podmínky stanovené právními předpisy k jeho používání, a že kupujícímu předá veškeré doklady potřebné k provozování předmětu koupě, za což kupujícímu ručí.
3. Předmětem koupě dle této smlouvy je dále:
   * doprava do místa plnění,
   * implementace, tj. veškeré nezbytné práce jejichž smyslem je zprovoznění včetně zapojení do stávajícího prostředí kupujícího tak, aby je kupující mohl užívat obvyklým způsobem (dále jen „implementace“),
   * předání průvodní dokumentace,
   * zaškolení kupujícího
   * součinnost při auditu kybernetické bezpečnosti a odstranění chyb bránící užívání dle účelu smlouvy zjištěných při testech
   * nezbytná technická podpora po dobu udržitelnosti Projektu, která činí 5 let od data předání do provozu. Technická podpora zahrnuje zejména aktualizace SW firewallu, maintenance, legislativní upgrade a update (dále jen „technická podpora“).

**4. Kupní cena a platební podmínky**

1. Celková kupní cena činí:

**………………………… Kč bez DPH**

**………………………… Kč DPH**

**………………………… Kč vč. DPH**

1. Cena bez DPH podle čl. 4.1. této smlouvy je stanovena dle technické specifikace (Příloha č. 1 této smlouvy) v souladu s jednotkovými cenami, uvedenými v položkovém rozpočtu (Příloha č. 2 této smlouvy) jako cena nejvýše přípustná a konečná a zahrnuje celý předmět plnění dle této smlouvy (s výjimkou ceny za poskytování technické podpory, která je upravena v čl. 4.5. níže).
2. Sjednaná cena celkem může být změněna pouze v případě změny zákona č. 235/2004 Sb., o DPH, týkající se sazby DPH a v souvislosti s ustanoveními § 222 zákona č. 134/2016 Sb., o zadávání veřejných zakázek.
3. Kupující se zavazuje zaplatit kupní cenu na základě faktur, vystavených prodávajícím a doručených kupujícímu dle níže uvedeného mechanismu:
   * 1. faktura ve výši 30 % z celkové kupní ceny dle čl. 4.1. výše bude vystavena po dodání zboží.
   * 2. faktura ve výši 40 % z celkové kupní ceny dle čl. 4.1. výše bude vystavena po zahájení auditu kybernetické bezpečnosti.
   * 3. faktura ve výši 30 % z celkové kupní ceny dle čl. 4.1. výše bude vystavena po oboustranném podpisu předávacího protokolu (tj. po předání a převzetí zboží do plného provozu).
4. Cena za technickou podporu po předání zboží do provozu je stanovena dohodnou smluvních strany na:

**………………………… Kč bez DPH za 1 měsíc**

**………………………… Kč DPH**

**………………………… vč. DPH za 1 měsíc**

1. Úhrada ceny za technickou podporu bude probíhat na základě měsíčně vystavované faktury. Datum uskutečnitelného zdanitelného plnění je sjednáno na poslední kalendářní den v měsíci.
2. Každá faktura musí splňovat náležitosti daňového dokladu podle § 28 zákona č. 235/2004 Sb., o DPH, bude obsahovat číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt* ***„Zvýšení kybernetické bezpečnosti pro infrastrukturu města Šlapanice“, reg. č. CZ.31.2.0/0.0/0.0/23\_093/0008390****, je spolufinancován z Národního plánu obnovy“* a bude zaslána prodávajícím na adresu kupujícího. **Splatnost faktury činí 30 kalendářních dní.**
3. Kupující bude oprávněn před uplynutím lhůty splatnosti vrátit prodávajícímu bez zaplacení fakturu, která nebude obsahovat některou náležitost uvedenou v této smlouvě, případně bude mít jiné závady v obsahu nebo bude uvedeno bankovní spojení a číslo účtu prodávajícího v rozporu s touto smlouvou anebo tyto náležitosti budou uvedeny chybně. U vrácené faktury musí kupující vyznačit důvod vrácení. Prodávající je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. Kupujícímu vrácením faktury přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží znovu ode dne doručení opravené nebo nově vyhotovené faktury kupujícímu.
4. Platby budou zásadně probíhat bezhotovostní formou na bankovní účet prodávajícího uvedený ve smlouvě. Změnu bankovního spojení a čísla účtu prodávajícího bude možno provést pouze písemným dodatkem k této smlouvě nebo písemným sdělením prokazatelně doručeným kupujícímu, nejpozději spolu s příslušnou fakturou.
5. Faktura se považuje za včas uhrazenou, pokud je fakturovaná částka odepsána z účtu kupujícího.

### 5. Místo a doba plnění a dodací podmínky

1. Místem plnění je sídlo kupujícího.
2. Prodávající je povinen dodat zboží **nejpozději do 90 dní od účinnosti této smlouvy**.
3. Dodávka se považuje podle této smlouvy za dodanou, pokud bylo:
   * zboží řádně dodáno včetně příslušné dokumentace (k instalaci, nastavení, zabezpečení jednotlivých komponent a včetně návrhu plánu obnovy).
   * provedena instalace, implementace (případné podrobné specifické podmínky implementace jsou uvedeny u jednotlivých zařízení v příloze č. 1 smlouvy) a úspěšně vyzkoušena funkčnost,
     + činnost u níž se nepředpokládá žádný výpadek služeb lze provádět v pracovní době MÚ,
     + činnost u které se obě strany shodnou že předpokládaný výpadek bude kratší než 10 min lze provádět mimo úřední hodiny,
     + činnosti s výpadkem delší se mohou provádět pouze mimo pracovní dobu MÚ. Termín odstávky musí být znám alespoň týden předem,
     + termín školení uživatelů min. měsíc předem,
     + školení OIT může probíhat v průběhu instalace.
   * součástí instalace bude následný testovací provoz provedený bez zbytečného odkladu v délce nutné pro ověření funkčnosti dodaného HW a SW. Náplň testovacího provozu bude následující:
     + zahoření a ověření funkčnosti HW zařízení
     + ověření vzájemné spolupráce jednotlivých HW zařízení
     + ověření napojení na LAN síť kupujícího
     + provedení zátěžových testů
     + ověření chování systému při výpadku některého ze zařízení (ověření vysoké dostupnosti)
     + ověření chování systému při výpadku el. energie
4. Po dodání zboží bude následovati **implementace částí 3, 4, 5, 6 zakázky**, bude dokončena **analýza rizik a zranitelností** včetně doplnění dokumentace systému řízení kybernetické bezpečnosti podle doporučení NUKIB **(tj. část 1 zakázky)** a rovněž proběhne **audit kybernetické bezpečnosti**.
5. V rámci auditu kybernetické bezpečnosti dojde k prověření funkčnost technických opatření a celkové bezpečnosti dodávky pomocí jejího otestování. Otestování provede 3. osoba zvolená kupujícím, přičemž toto otestování bude trvat maximálně 60 dní. V návaznosti na dokončení auditu kybernetické bezpečnosti prodávající napraví nalezené chyby bránící užívání dle účelu smlouvy, a to nejpozději do 14 dní od okamžiku, kdy obdrží výsledek auditu kybernetické bezpečnosti.
6. Po splnění dodávky zboží, tj. po prodávající napraví chyby bránící užívání dle účelu smlouvy nalezené v rámci auditu kybernetické bezpečnosti, bude vyhotoven **zápis o předání a převzetí zboží**, který bude obsahovat níže uvedené náležitosti:
   * název a sídlo prodávajícího a kupujícího,
   * označení dodaného zboží včetně výrobního čísla,
   * datum dodání,
   * číslo a název dotačního projektu

(konkrétně bude uveden text ve znění: *Projekt* ***„Zvýšení kybernetické bezpečnosti pro infrastrukturu města Šlapanice“, reg. č. CZ.31.2.0/0.0/0.0/23\_093/0008390*** *je spolufinancován z Národního plánu obnovy“*).

1. Zápis o předání a převzetí zboží podepíší oprávnění zástupci obou smluvních stran, přičemž podpisem zápisu o předání a převzetí dochází k převzetí a předání zboží a ke splnění předmětu koupě.

### 6. Odpovědnost za vady, záruka za jakost, servis

1. Prodávající nese odpovědnost za to, že zboží dodané a předané podle této smlouvy je ke dni dodání plně funkční a splňuje technické parametry uvedené této smlouvě. Prodávající přejímá níže uvedenou záruku za jakost zboží dodaného podle této smlouvy. Záruční doba počíná běžet dnem oboustranného podpisu zápisu o předání a převzetí zboží. **Záruční doba pro jednotlivé položky v souladu s přílohou č. 1 této smlouvy činí 60 měsíců** ode dne předání a převzetí zboží.
2. Záruka se nevztahuje na spotřební materiál a na vady způsobené zaviněným jednáním kupujícího anebo způsobené vyšší mocí.
3. Kupující se zavazuje respektovat pokyny prodávajícího v oblasti údržby a používání správných pracovních postupů.
4. Technická podpora a servis budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. min. 60 měsíců ode dne předání do provozu).
5. Technická podpora a servis budou realizovány v sídle kupujícího. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.
6. V případě nahlášení závady prodávajícímu bude oprava provedena vzdáleně či na místě nejpozději následující pracovní den od jejího nahlášení. V případě nemožnosti opravy následující pracovní den nabídne prodávající kupujícímu alternativu (tj. náhradní řešení) na dobu trvání opravy. V případě záruční opravy (tj. pokud se nejedná o vadu způsobenou zaviněným jednáním kupujícího anebo způsobenou vyšší mocí), není kupující povinen hradit náklady na cestovné servisních techniků ke kupujícímu a zpět, tyto náklady nese prodávající.
7. Nahlášení závady bude provedeno prostřednictvím e-mailu zaslaného na e-mailovou adresu……...[[1]](#footnote-1), telefonicky na tel. číslo ……...[[2]](#footnote-2), prostřednictvím elektronické oznamovací služby (tzv. HelpDesku) nebo prostřednictvím vzdáleného připojení na PC uživatele / server.
8. Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 8 do 16 hod.
9. Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).
10. Prodávající se v záruční době zavazuje zajistit dostupnost náhradních dílů a spotřebního materiálu.
11. Po dobu běhu záruční doby bude zajištěna udržitelnost HW a SW včetně třetích stran.
12. Technická podpora a servis zařízení HW a SW budou realizovány přímo prodávajícím, případně prostřednictvím autorizovaného servisního kanálu výrobce.

**7. Smluvní pokuta a úrok z prodlení**

1. Smluvními stranami bylo ujednáno, že pokud bude kupující v prodlení s úhradou ceny plnění ujednané podle této smlouvy, je kupující povinen zaplatit úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i započatý kalendářní den prodlení.
2. Ocitne-li se prodávající v prodlení s plněním podle této smlouvy dle čl. 5.2, je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny, a to za každý, byť i započatý kalendářní den prodlení se splněním dodávky.
3. Ocitne-li se prodávající v prodlení s plněním podle této smlouvy dle čl. 5.5 (tj. pokud nenapraví nalezené chyby bránící užívání dle účelu smlouvy zjištěné v rámci auditu kybernetické bezpečnosti ve stanovené lhůtě), je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny, a to za každý, byť i započatý kalendářní den prodlení se splněním dodávky.
4. Ocitne-li se prodávající v prodlení s plněním dle čl. 6.6. této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši 500,- Kč za každý započatý den prodlení s dokončením servisní opravy dle čl. 6.6.
5. Uplatněním nároku na smluvní pokutu dle této smlouvy není dotčen nárok na náhradu škody.
6. Smluvní pokuta je splatná ve lhůtě 30 dnů od doručení jejího vyúčtování povinné smluvní straně z této smluvní pokuty.

### 8. Doba trvání smlouvy, ukončení smlouvy

1. Tato smlouva se uzavírá na dobu určitou, nejdéle do doby splnění závazku dle této smlouvy (tj. do okamžiku ukončení poskytování nezbytné technické podpory, resp. do doby uplynutí 5 let od data předání zboží do provozu).
2. Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy, přičemž za podstatné porušení této smlouvy se zejména považuje:
   1. na straně kupujícího – nezaplacení kupní ceny podle této smlouvy ve lhůtě delší 14 dní po dni splatnosti příslušné faktury,
   2. na straně prodávajícího – prodlení s dodáním zboží o více než 14 dní po termínu dodání dle čl. 5.2. či dodání nefunkčního zboží, nesplňujícího požadavky čl. 3 této smlouvy, marné uplynutí sjednané lhůty pro vyřízení záruční opravy dle čl. 6.6.
3. Smluvní strana porušením povinnosti dotčená je povinna odstoupení od smlouvy písemně oznámit druhé smluvní straně.

### 9. Ostatní ujednání

1. Smluvní strany se dohodly, že vlastnické právo k dodanému předmětu smlouvy nabývá kupující okamžikem převzetí zboží od prodávajícího.
2. Nebezpečí škody na zboží přechází z prodávajícího na kupujícího okamžikem převzetí zboží od prodávajícího či okamžikem, kdy kupujícímu bylo umožněno zboží převzít a ten jej nepřevzal.
3. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých vzájemných závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.
4. Smluvními stranami bylo ujednáno, že veškeré informace, jež si navzájem poskytnou, jsou označeny jako důvěrné a žádná ze smluvních stran není oprávněna je poskytnout třetí osobě ani použít v rozporu s jejich účelem pro své potřeby.
5. Prodávající nesmí bez předchozího souhlasu kupujícího postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.
6. Kupující se zavazuje umožnit přístup určeným pracovníkům prodávajícího do prostoru svého objektu za účelem splnění této smlouvy (předání a převzetí zboží, servis a technická podpora).
7. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku a dalšími právními předpisy České republiky.
8. Ujednává se, že případné spory vzniklé z této smlouvy budou účastníci řešit především vzájemnou dohodou. Pro řízení o případných sporných nárocích se ujednává příslušnost soudů. Rozhodným právem je právo České republiky.
9. Za písemnou formu výzvy nebo oznámení se pro účely této smlouvy pokládají oznámení učiněná elektronickou poštou na dohodnuté elektronické adresy.
10. Prodávající je povinen zajistit, že veškeré vlastnosti předmětu smlouvy, včetně jeho update, legislativních update, upgrade a legislativních upgrade budou po celou dobu účinnosti této smlouvy odpovídat obecně platným právním předpisům ČR.
11. Prodávající prohlašuje, že bude mít po celou dobu plnění předmětu smlouvy uzavřenu pojistnou smlouvu kryjící odpovědnost za škodu způsobenou provozní činností s limitem pojistného plnění minimální výši kupní ceny zboží dle čl. 4.1., kterou se zavazuje kdykoliv na vyžádání předložit k nahlédnutí kupujícímu.

### 10. Závěrečná ustanovení

1. Prodávající je povinen umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů).
2. Prodávající je povinen uvádět povinné prvky publicity podle podmínek strukturálních fondů EU na všech tištěných dokumentech vytvořených v souvislosti s předmětem koupě (nevztahuje se na interní účetní dokumentaci apod.). Tyto povinné prvky publicity sdělí a poskytne prodávajícímu na vyžádání kupující.
3. Prodávající je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. **Prodávající je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinou spolupůsobit při výkonu finanční kontroly.**
4. Prodávající se zavazuje umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je veřejná zakázka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu nejméně 10 let od ukončení financování díla způsobem, který je v souladu s platnými právními předpisy České republiky a Evropských společenství.
5. Prodávající je povinen minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací projektu, z něhož je Veřejná zakázka hrazena, zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
6. Prodávající bere na vědomí, že úhrada ceny za předmět plnění bude provedena s využitím dotačních prostředků, získaných kupujícím a podléhajících kontrole z hlediska vykazování účelnosti jejich čerpání. Prodávající se zavazuje, že kupujícímu nahradí veškeré škody a náklady, které mu vzniknou nebo budou muset být vynaloženy, pokud z důvodu porušení této smlouvy prodávajícím vznikne kupujícímu závazek vrátit dotaci nebo její část, poskytnutou na úhradu ceny za předmět plnění, jejímu poskytovateli, a to i včetně penále případně vyměřeného jako důsledek porušení pravidel nakládání s veřejnými prostředky. To platí obdobně, pokud prodávající znemožní řádný výkon kontroly orgánům, oprávněným ke kontrole účelnosti vynaložení dotačních prostředků, resp. nepředloží jimi požadované doklady.
7. Prodávající se zavazuje k dodržování mezinárodních sankcí Evropské unie, přijatých v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku, zejména nařízení Rady EU č. 2022/576, nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č. 2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch (dále jen „mezinárodní sankce EU“).
8. Prodávající se zavazuje během plnění smlouvy i po jejím ukončení smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od kupujícího v souvislosti s plněním smlouvy
9. Tuto smlouvu lze měnit nebo doplnit pouze dohodou smluvních stran, a to formou písemného číslovaného dodatku.
10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně.
11. Smlouva je, v souladu s podmínkami zákona č. 134/2016 Sb., podepsána elektronicky.
12. Doložka podle § 41 zák. č. 128/2000 Sb., o obcích, v platném znění. Tuto kupní smlouvu na „dodávku infrastruktury“, ev. č. XXX/2025, schválila Rada města Šlapanice na svém XX. zasedání konaném dne xx. xx. xxxx.
13. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem jejího uveřejnění v registru smluv. Uveřejnění smlouvy v registru smluv provede kupující.
14. Nedílnou součástí této smlouvy jsou následující přílohy:

**Příloha č. 1 – Technická specifikace**

**Příloha č. 2 – Položkový rozpočet**

Prodávající: Kupující:

V …………………dne dle data el. podpisu Ve Šlapanicích dne dle data el. podpisu

………………………………… …………………………………

Jméno a Příjmení Mgr. Michaela Trněná, starostka

Funkce Město Šlapanice

**Příloha č. 1 – Technická specifikace[[3]](#footnote-3)**

Zabezpečení komunikační sítě a segmentace sítě

**Switch PoE 5ks**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: L2 switch | ano |  |
| Formát zařízení do racku | ano |  |
| Maximální velikost zařízení: 1U | ano |  |
| Počet 1Gbit/s metalických portů | min. 48×RJ45 |  |
| Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním | min. 4×SFP+ |  |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery | ano |  |
| Všechny ethernet porty jsou dostupné zepředu | ano |  |
| Interní napájecí zdroj | ano |  |
| Podpora PoE+ dle standardu 802.3at | ano |  |
| Dostupný výkon pro PoE+ napájení | min. 740W |  |
| Podpora Energy Efficient Ethernet (802.3az) | ano |  |
| Celková propustnost přepínače | min. 176 Gb/s |  |
| Celkový paketový výkon přepínače | 98 mpps |  |
| Minimální paketový buffer: 12 MB | ano |  |
| Maximální přípustná hloubka přepínače | max. 33cm |  |
| **Základní funkce a protokoly** |  |  |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte | ano |  |
| Podpora linkové agregace IEEE 802.3ad | ano |  |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4 | ano |  |
| Minimální počet LACP skupin/linek ve skupině: 8/8 | ano |  |
| Protokol pro definici šířených VLAN: MVRP | ano |  |
| Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN | ano |  |
| IEEE 802.1s - Multiple Spanning Tree | ano |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) | ano |  |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | ano |  |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace | ano |  |
| Statické směrování IPv4 a IPv6 | ano |  |
| IGMP v2 a v3 | ano |  |
| MLD v1 a v2 | ano |  |
| Hardware podpora IPv4 a IPv6 ACL | ano |  |
| ACL definice na základě skupiny fyzických portů | ano |  |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN | ano |  |
| BPDU guard a Root guard | ano |  |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps | ano |  |
| ICMPv4 a ICMPv6 rate-limiting per port | ano |  |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port | ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou) | ano |  |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN | ano |  |
| Dynamické zařazování do VLAN | ano |  |
| 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) | ano |  |
| Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC | ano |  |
| Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení | ano |  |
| Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC | ano |  |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU | ano |  |
| Podpora IPv4 a IPv6 QoS | ano |  |
| Minimálně 8 front pro IEEE 802.1p | ano |  |
| **Management** |  |  |
| CLI formou 1x USB-C console port | ano |  |
| Konfigurace zařízení v člověku čitelné textové formě | ano |  |
| Podpora automatických i manuálních snapshotů konfigurace systému | ano |  |
| USB port pro diagnostiku, přenos konfigurace a firmware | ano |  |
| Podpora managementu přes IPv4 i IPv6 | ano |  |
| Podpora SSHv2 server, HTTPS server a SFTP klient | ano |  |
| Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DHG15 nebo vyšší | ano |  |
| Podpora SNMPv2c a SNMPv3 | ano |  |
| RMON | ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |  |
| Lokálně vynucené RBAC na úrovni přepínače | ano |  |
| Dualní flash image | ano |  |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů | ano |  |
| Podpora SYSLOG over TLS | ano |  |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování | ano |  |
| Podpora RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec | ano |  |
| Podpora TACACS+ včetně command authorization | ano |  |
| Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler) | ano |  |
| Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem | ano |  |
| Analýza síťového provozu sFlow podle RFC 3176 | ano |  |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session | ano |  |
| Podpora Zero Touch Provisioning (ZTP) | ano |  |
| REST API pro automatizaci nastavení | ano |  |
| Automatická konfigurace portu podle připojeného zařízení | ano |  |
| Podpora Cloud based management | ano |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ano |  |

**Switch 21ks**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: L2 switch | ano |  |
| Formát zařízení do racku | ano |  |
| Maximální velikost zařízení: 1U | ano |  |
| Počet 1Gbit/s metalických portů | 48×RJ45 |  |
| Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním | 4×SFP+ |  |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery | ano |  |
| Všechny ethernet porty jsou dostupné zepředu | ano |  |
| Interní napájecí zdroj | ano |  |
| Podpora Energy Efficient Ethernet (802.3az) | ano |  |
| Celková propustnost přepínače | 176 Gb/s |  |
| Celkový paketový výkon přepínače | 98 mpps |  |
| Minimální paketový buffer: 12 MB | ano |  |
| Maximální přípustná hloubka přepínače | max. 25cm |  |
| **Základní funkce a protokoly** |  |  |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte | ano |  |
| Podpora linkové agregace IEEE 802.3ad | ano |  |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4 | ano |  |
| Minimální počet LACP skupin/linek ve skupině: 8/8 | ano |  |
| Protokol pro definici šířených VLAN: MVRP | ano |  |
| Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN | ano |  |
| IEEE 802.1s - Multiple Spanning Tree | ano |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) | ano |  |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | ano |  |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace | ano |  |
| Statické směrování IPv4 a IPv6 | ano |  |
| IGMP v2 a v3 | ano |  |
| MLD v1 a v2 | ano |  |
| Hardware podpora IPv4 a IPv6 ACL | ano |  |
| ACL definice na základě skupiny fyzických portů | ano |  |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN | ano |  |
| BPDU guard a Root guard | ano |  |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps | ano |  |
| ICMPv4 a ICMPv6 rate-limiting per port | ano |  |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port | ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou) | ano |  |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN | ano |  |
| Dynamické zařazování do VLAN | ano |  |
| 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) | ano |  |
| Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC | ano |  |
| Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení | ano |  |
| Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC | ano |  |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU | ano |  |
| Podpora IPv4 a IPv6 QoS | ano |  |
| Minimálně 8 front pro IEEE 802.1p | ano |  |
| **Management** |  |  |
| CLI formou 1x USB-C console port | ano |  |
| Konfigurace zařízení v člověku čitelné textové formě | ano |  |
| Podpora automatických i manuálních snapshotů konfigurace systému | ano |  |
| USB port pro diagnostiku, přenos konfigurace a firmware | ano |  |
| Podpora managementu přes IPv4 i IPv6 | ano |  |
| Podpora SSHv2 server, HTTPS server a SFTP klient | ano |  |
| Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DHG15 nebo vyšší | ano |  |
| Podpora SNMPv2c a SNMPv3 | ano |  |
| RMON | ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |  |
| Lokálně vynucené RBAC na úrovni přepínače | ano |  |
| Dualní flash image | ano |  |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů | ano |  |
| Podpora SYSLOG over TLS | ano |  |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování | ano |  |
| Podpora RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec | ano |  |
| Podpora TACACS+ včetně command authorization | ano |  |
| Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler) | ano |  |
| Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem | ano |  |
| Analýza síťového provozu sFlow podle RFC 3176 | ano |  |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session | ano |  |
| Podpora Zero Touch Provisioning (ZTP) | ano |  |
| REST API pro automatizaci nastavení | ano |  |
| Automatická konfigurace portu podle připojeného zařízení | ano |  |
| Podpora Cloud based management | ano |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ano |  |

**Ostatní podmínky:**

* Oba typy switchů musí být od stejného výrobce a ze stejné modelové řady
* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
* Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
* Součástí dodávky je 104 ks SFP+ SW pro výše uvedené switche
* Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.
* Je požadovaná technická podpora výrobce po dobu 60 měsíců.
* Prodávající je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

|  |  |
| --- | --- |
| **Ověřování zařízení - AP** | **splněno ANO/NE** |
| ***základní technické požadavky*** | |
| Vnitřní přístupový bod v počtu kusů 25 |  |
| Podpora bezdrátových standardů: 802.11a/b/g/n/ac/ax |  |
| Certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED 6E™ a WPA3™ Enterprise |  |
| Pracovní režim AP řízené kontrolérem (lightweight) |  |
| Kontroler musí být on-prem, řízení z cloud kontroleru je nepřípustné. Nejde-li využít stávající kontrolery zadavatele v HA zapojení, musí být součástí dodávky 2 kontrolery v HA zapojení. |  |
| Minimální počet portů ethernet LAN: 1x 100/1000/2500 Mbit/s RJ45 |  |
| Podpora linkové agregace LACP |  |
| Bezvýpadkový (hitless) PoE failover mezi ethernetovými porty |  |
| Podpora standardního PoE+ IEEE 802.3at 30W bez nutnosti redukce výkonu libovolného rádia |  |
| Podpora napájení z AC napájecího zdroje |  |
| Rozsah provozních teplot 0° až +50°C bez redukce vysílacího výkonu nebo omezení funkcí |  |
| Ochrana proti přehřátí - vestavěný teplotní senzor, který automaticky krátkodobě vypne AP |  |
| Vestavěná interní anténa MIMO, omni down-tilt |  |
| Radiová část: tri-band, současná podpora pásem 2.4GHz, 5GHz a 6GHz |  |
| Minimální MIMO a počet spatial stream: 2x2 |  |
| Podpora TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax |  |
| HW podpora OFDMA |  |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP |  |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 6GHz: 2400 Mbps, pro 5GHz: 1200 Mbps a pro 2.4GHz: 500 Mbps |  |
| Integrovaný TPM pro bezpečné uložení certifikátů |  |
| Podpora 802.11ac explicitního beamformingu |  |
| Podpora airtime fairness |  |
| Prioritizace jednotlivých SSID na základě vysílacího času |  |
| Vypínatelné indikační LED diody informující o stavu zařízení |  |
| Prioritizace 6GHz a 5GHz pásma – Band Steering či obdobné |  |
| Automatická detekce Rogue AP |  |
| Nastavitelný DTIM interval pro jednotlivé SSID |  |
| Podpora WPA3-CNSA, WPA3-SAE, OWE |  |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |  |
| VLAN Pooling |  |
| Podpora wireless MESH s protokolem pro optimální výběr cesty v rámci MESH stromu |  |
| Podpora Layer-2 izolace bezdrátových klientů |  |
| HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu) |  |
| Hardware filtry proti intermodulačnímu rušení pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) |  |
| Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček |  |
| DHCP server, směrování a NAT pro bezdrátové klienty |  |
| AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN |  |
| Automatická identifikace připojeného zařízení a jeho operačního systému |  |
| Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming |  |
| Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP |  |
| Optimalizace provozu: multicast-to-unicast konverze |  |
| Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace) |  |
| Podpora filtrování přístupu na web |  |
| Podpora RadSec (RADIUS over TLS) |  |
| 802.11w ochrana management rámců |  |
| Podpora Kensington lock |  |
| Podpora MAC ověřování a 802.1X autentizace Wi-Fi klientů s využitím lokální databáze v AP |  |
| AP se ověřuje před připojením do LAN pomocí 802.1X - podpora PEAP a EAP-TLS suplicant |  |
| CLI formou serial konsole port a serial over Bluetooth |  |
| SSHv2, SNMPv2c a SNMPv3 |  |
| Integrované Bluetooth Low Energy (BLE) rádio |  |
| Integrované Zigbee 802.15.4 rádio |  |
| Podpora režimu SLEEP |  |
| Součástí AP je příslušenství pro montáž na zeď nebo strop |  |
| Standardní záruka výrobce zařízení min. 5 let v sídle zadavatele |  |

|  |  |
| --- | --- |
| **NAC - ověřování uživatelů a zařízení** | **splněno ANO/NE** |
| ***požadavky*** | |
| Virtuální appliance pro platformu VMware ESX verze 7 a vyšší nasazená on-prem v prostředí zadavatele |  |
| Možnost instalace VM v prostředí AWS či Azure s podporou HA režimu |  |
| Podpora distribuované architektury s centrálním prvkem správy |  |
| Autentizační brány musí být nasazené mimo samotný datový tok |  |
| Podpora HA v režimu active-passive |  |
| Sdílení licencí v HA režimu active-passive |  |
| Nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky |  |
| Komunikace se síťovými prvky (drátovými i bezdrátovými) pomocí SNMP a CLI, i u jiných výrobců |  |
| Vymáhání definovaných bezpečnostních politik bez nutnosti využití 802.1x nebo MAB |  |
| Možnost instalace samostatného NAC řešení bez nutnosti nákupu dalších prvků (např. centrální management). Pokud je další prvek nutný, musí být součástí nabídky na NAC |  |
| Autentizační brána poskytuje služby DHCP a DNS pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě |  |
| Řešení funguje samo o sobě jako Radius server pro autentizaci i accounting |  |
| Správa řešení pomocí SSH, CLI a HTTPS |  |
| Možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů |  |
| Autentizace a bezpečnostní kontrola koncového zařízení před jeho připojením do sítě nezávisle na způsobu připojení (LAN, WiFi, VPN) |  |
| Detailní profilace připojeného zařízení a klienta buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externím systémy |  |
| Podpora politik pro automatickou profilaci zařízení, minimálně dle: SNMP, Radius, Syslog, DHCP, API, SSH, Nmap, HTTP/S, IP range, telnet, vyhodnocení TCP/UDP portů, Vendor OUI/MAC, WMI profil |  |
| Periodická kontrola připojeného zařízení, zda stále odpovídá profilu, na základě kterého bylo vpuštěno do sítě a možnost jeho odpojení v případě, že nesplňuje podmínky původního profilu |  |
| Podporované autentizační protokoly MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS |  |
| Po úspěšné autentizaci možnost definice parametrů síťového portu či SSID pomocí standardních Radius atributů |  |
| Po úspěšné autentizaci je možné na síťové zařízení instalovat z NAC brány konfiguraci, např. ACL |  |
| Podpora 802.1x |  |
| Podpora MAB autentizace |  |
| Podpora tvorby lokálních účtů a lokální autentizace |  |
| Podpora registrace koncových zařízení v NAC před jejich fyzickým připojením do sítě |  |
| Podpora funkce Radius Proxy |  |
| Možnost integrace se stávající certifikační autoritou (CA) |  |
| Podpora agentů pro operační systémy Windows, MacOS, Linux. Licence pro tyto agenty je součástí dodané licence NAC |  |
| Podpora integrace se stávajícím Active Directory serverem pro autentizaci uživatelů pomocí LDAP |  |
| Podpora CAPTIVE portálu v rámci autentizační brány s plně editovatelným prostředím |  |
| Nejméně 5 různých CAPTIVE portálů z důvodu velikosti prostředí |  |
| V případě zjištění bezpečnostního incidentu je řešení schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovni vrstvy L2 |  |
| Podpora integrace s MDM nástroji (např. MS In-Tune) |  |
| Podpora integrace s poptávaným firewallem a analytickým řešením nad provozem poptávaného firewallu i NAC |  |
| Uživatel s oprávněním administrátora má možnost ručně registrovat, zablokovat nebo smazat nové zařízení nebo uživatele |  |
| Kontrola pravidel se provádí před povolením přístupu do sítě na základě profilu nebo agenta na koncovém zařízení |  |
| Kontrolu je možné provádět periodicky, pokud je zařízení připojeno do sítě |  |
| Kontrola stavu registrů |  |
| Kontrola stavu antiviru na stanici |  |
| Kontrola existence konkrétních souborů v lokálním systému |  |
| Ověření domény |  |
| Ověření verze a úrovně aktualizací na operačním systému |  |
| Možnost sběru informací o instalovaných aplikacích na stanici |  |
| Upozornění uživatele v případě nesplnění bezpečnostní kontroly, případně s přesměrováním na CAPTIVE portál |  |
| Možnost odeslání zprávy na koncovou stanici v případě nasazení agenta |  |
| Ověření certifikátu a jeho atributů (vydavatele, expirace, common-name a dalších |  |
| Řešení je možné ovládat i pomocí výrobcem popsaných API, které musí být dostupné v manuálech či dokumentaci na stránkách výrobce |  |
| Dostupnost a možnost tvorby reportů o stavu platformy a připojených zařízení v reálném čase a zpětně alespoň o jeden týden |  |
| Všechny požadované funkce pokrývá jeden typ licence, je možné dodatečně dokoupit další licence |  |
| Perpetual(nikoli předplatné) licence pro 500 současně připojených zařízení |  |
| Podpora výrobce v režimu 24/7 na systém i konfiguraci, po dobu 5-ti let |  |

|  |  |
| --- | --- |
| **Analýza a ukládání logů** | **Splněno ANO/NE** |
| ***základní technické požadavky*** | |
| nástroj pro bezpečnostní analýzu logů z NGFW zařízení se schopností jejich korelace včetně možnosti ukládání logů |  |
| podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení |  |
| virtuální appliance pro platformu VMWare, Microsoft Hyper-V, KVM (fyzické zařízení není přípustná laternativa) |  |
| možnost nativní integrace s poptávaným zařízením typu NGFW, které bude sloužit jako zdroj dat pro analýzu |  |
| alespoň 5TB alokovatelná kapacita dlouhodobého úložiště logů a alespoň 6GB minimální limit pro množství přijatých logů k analýze za jeden den (možnost navýšení limitů pomocí dodatečné licence) |  |
| minimálně 4x vNIC |  |
| možnost provozovat poptávané řešení jako prosté uložiště logů z dalších zařízení zákazníka bez jejich další analýzy |  |
| možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje |  |
| možnost generovat reporty na základě specifikace dotazů do databáze logů poptávaného řešení |  |
| HTML/CSV/XML/PDF fortmát generovaných reportů s možností plánování pravidelné automatické tvorby reportů |  |
| možnost logické segmentace s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat |  |
| musí obsahovat předdefinované vzory reportů a umožňovat úpravu vzhledu generovaných reportů prvky zákazníka (loga, hlavička, …) |  |
| možnost zobrazení aktuálních logů z jednotlivých integrovaných NGFW zařízení v reálném čase |  |
| možnost zpětného zobrazení a analýzy logů z důvodu možnosti zpětné analýzy provozu a možných uskutečněných bezpečnostních hrozeb |  |
| ***požadavky na management*** | |
| plnohodnotná správa pomocí grafického rozhraní a CLI |  |
| podpora SNMPv2 a SNMPv3 a REST API |  |
| samostatná sekce v grafickém rozhraní pro zobrazní zjištěných hrozeb |  |
| podpora přijímání syslogů ze zařízení třetích stran |  |
| možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením |  |
| ***další požadavky*** | |
| podpora výrobce v režimu 24/7 na dobu min. 5 let |  |
| všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu min. 5 let musí být také součástí dodávky |  |

|  |  |
| --- | --- |
| **Firewall HA cluster** | **splněno ANO/NE** |
| ***základní technické požadavky*** | |
| 2x HW appliance o velikosti 1 RU v režimu vysoké dostupnosti (active-active, active-passive) |  |
| grafické konfigurační rozhraní a příkazový řádek |  |
| min. 12 metalických RJ-45 portů 10/100/1000 |  |
| min. 4 optická datová rozhraní SFP+ o rychlosti 10Gb/s |  |
| min. 4 optická datová rozhraní SFP o rychlosti 1Gb/s |  |
| 1 dedikovaný port pro správu pomocí konzole pro přístup k CLI a 1 management port |  |
| NGFW musí podporovat plnohodnotnou inspekci sítového provozu v režimech: |  |
| NAT/router |  |
| L2 transparentní režim (dva a více sítových rozhraní) |  |
| L2 interface pair (dvě sítové rozhraní) |  |
| Redudantní napájení firewallu |  |
| ***výkonové požadavky*** | |
| Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 35 Gbps (UDP pakety o velikosti 512 B) |  |
| Nízké vložené zpoždění zařízení (latence) max. 5μs |  |
| Minimální počet současně navázaných spojení firewallu 2.5 M |  |
| Minimální počet nových spojení za sekundu 120 k |  |
| Propustnost firewallu v packetech min. 40 Mpps |  |
| Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) minimálně 3 Gbps |  |
| Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 2.5 Gbps |  |
| Propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 5 Gbps |  |
| Propustnost funkce rozpoznávání sítových aplikací na L7 min. 5 Gbps |  |
| Propustnost IPSEC VPN v konfiguraci AES256/SHA256 min. 30 Gbps |  |
| Propustnost funkce SSL inspekce provozu min. 2.7 Gbps |  |
| Min. počet konfigurovatelných virtuálních kontextů na každém zařízení 10 |  |
| ***funkční požadavky*** | |
| Funkce rozpoznávání kancelářských aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací |  |
| Funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min. 10 000 signatur v databázi; podpora zabezpečení kancelářských (IT) |  |
| Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předání zkoumaných souborů pro analýzu v prostředí typu sandbox |  |
| funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze |  |
| funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek |  |
| Výjimka z SSL inspekce na základě administrátorem definovaných adres |  |
| Výjimka z SSL inspekce na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.) |  |
| Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On |  |
| Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky |  |
| Funkce QoS, traffic shaping |  |
| Funkce klientské VPN (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál, možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů |  |
| Site-to-Site IPsec VPN s podporou statického i dynamického routování |  |
| Podpora DLP pro identifikaci, monitorování a ochranu dat |  |
| Podpora IoT protokolů (minimálně klasifikace provozu, identifikace zařízení, ochrana zařízení před sítovým útokem) |  |
| Podpora výrobce v režimu 24x7 a aktualizace všech požadovaných bezpečnostních funkcí po dobu 5 let |  |
| Umístění výrobce v Gartner MQ for Network Firewalls v sekci „Leaders“ v posledních 3 letech |  |

|  |  |
| --- | --- |
| **Mail gateway emailová ochrana** | **splněno ANO/NE** |
| ***základní technické požadavky*** | |
| virtuální řešení pro platformu VMWare, KVM a Microsoft Hyper-V |  |
| podpora režimu vysoké dostupnosti (A-A, A-P) - pokud je potřeba licence pro takové režimy fungování, musí být součástí dodávky |  |
| možnost nasazení v režimu gateway (MTA), server i transparent, licence pro všechny požadované režimy je součástí dodávky |  |
| certifikace řešení alespoň VBSpam a VB100 |  |
| možnost přidělení minimálně čtyř virtuálních síťových rozhraní |  |
| výkonové požadavky | |
| podpora alokovatelné diskové kapacity až 1TB |  |
| požadovaná propustnost řešení min. 30 000 email/h při využití souběžné inspekce pomocí antivirus a antispam profilů. referenční velikost kontrolovaného emailu je 100 kB. |  |
| v režimu server je možno vytvořit až 150 schránek, případná licence pro takový počet schránek je součástí nabízeného řešení |  |
| řešení je schopno konfigurovat pro ochranu až 20 domén, pro každou doménu je možné nastavit až 50 inspekčních profilů |  |
| ***funkční požadavky*** | |
| podpora IPv4 i IPv6 |  |
| podpora SMTP autentizace min. pomocí protokolů LDAP, RADIUS, POP3 a IMAP |  |
| integrovaná funkce antivirové ochrany emailového provozu s podporou real-time ochrany před outbrake škodlivého kódu, databáze antivirových signatur musí být udržována výrobcem nabízeného řešení a automaticky aktualizovaná |  |
| podpora nastavení limitů v rámci SMTP relací - počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstratení Received hlavičky) |  |
| schopnost analýzy PDF dokumentů v příloze kontrolované zprávy |  |
| shodné možnosti nastavení a provedení kontroly příchozí i odchozí komunikace |  |
| granulární konfigurace pravidel (pravidla na základě IP adres a/nebo domén příjemce, možnost využití wildcard notace) |  |
| možnost využití zabudované geo databáze IP adres v rámci pravidel, databáze musí být udržovaná výrobcem nabízeného řešení |  |
| podpora karantény s uživatelským přístupem umožnujícím běžné operace pomocí odděleného síťového rozhraní |  |
| podpora systémové karantény |  |
| podpora externího úložiště (šifrovaná komunikace, např. SFTP) |  |
| řešení a jeho dodané licence umožní provozovat TLS šifrování |  |
| řešení a jeho dodané licence umožní nastavit S/MIME |  |
| řešení a jeho dodané licence umožní nastavit DKIM, SPF a DMARC |  |
| řešení a jeho dodané licence umožní nastavit zabezpečení přenosu mailové komunikace pomocí IBE |  |
| funkce ochrany rate limiting, vyhodnocování lokálního skóre odesílatelů (na základě nedávné activity) s možností nastavení chování pro různé úrovně skóre |  |
| funkce zabezpečení dokumentů v příloze se schopností odstranění potencionálně nebezpečných prvků v dokumentu (makra, URL, …) včetně dokumentů MS Office a PDF při zachování typu dokumentu |  |
| automatická dekrypce šifrovaných dokumentů za pomoci administrátorem předdefinovaného slovníku hesel, za účelem provedení plné AV a AS kontroly |  |
| reakce na detekovanou hrozbu v podobě alespoň prřidání tagu, přidání nové hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce atd. |  |
| funkce opakované kontroly emailu ve chvíli jeho vyzvednutí z karantény |  |
| ochrana před škodlivými URL (výrobcem udržovaná databáze škodlivých URL), možnost uživatelské volby nežádoucích webových kategorií (phishing, malware, adult material, ...) |  |
| URL click protection a ochrana proti impersonifikaci |  |
| SandBox funkcionalita v prostředí výrobce řešení pro podporu detekce Zero Day hrozeb |  |
| ochrana před útoky typu BEC |  |
| architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty |  |
| ***požadavky na management*** | |
| plnohodnotná správa pomocí (HTTPs) a CLI (SSH) je součástí nabízeného řešení |  |
| možnost omezení administrátorských práv na definované domény |  |
| integrované logování systémových událostí a průběhu inspekce provozu s možností zobrazení logů v GUI |  |
| podpora protokolů SNMP (v2c, v3) a syslog pro možnost začlenění do externího monitorovacího systému |  |
| podpora logování na externí log server (syslog) |  |
| podpora archivace (přístup do archivu pomocí protokolu IMAP) |  |
| podpora REST API pro možnost integrace do stávající infrastruktury, případná licence musí být součástí dodávky |  |
| oddělení administrátorského a uživatelského přístupu do emailových schránek a karantény přes různá síťová rozhraní |  |
| ***další požadavky*** | |
| podpora výrobce v režimu 24/7 na dobu min. 5 let |  |
| všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu min. 5 let musí být také součástí dodávky |  |

**Compute servery**

**Specifikace serveru 3 kusy**

Je požadováno nové nepoužité zařízení určené pro český (EU) trh s uvedenými minimálními požadavky, které musí splňovat:

|  |  |
| --- | --- |
| **Server** | **Splněno ANO/NE** |
| Provedení do racku, barevně značené hot-plug vnitřní komponenty a místa pro uchopení |  |
| Výška max. 2U, šířka 19“, montáž do racku výsuvné lyžiny včetně ramene pro kabely |  |
| Trusted Platform Module 2.0 |  |
| Dvousocketový systém založený na Intel platformě (z důvodu kompatibility se současným clusterem). |  |
| Osazený 1x CPU s přesně 16 fyzickými jádry (z licenčních důvodů na serverech provozovaných systémů) o základní frekvenci min. 3.6 GHz. Výkon CPU Throughput SPECrate® 2017 Integer minimálně 195 Base pro 1 socket sestavu. Tento výsledek testu musí být dostupný přímo pro nabízený konkrétní model konkrétního výrobce serveru. |  |
| Požadovaná kapacita RAM minimálně 512 GB typu DDR5 5600MT/s složená z 8 dimm modulů. Musí umožnovat přidat min. dalších 512 GB paměti ve stejných modulech a kapacitě, bez nutnosti výměny původních modulů. |  |
| **Diskový subsystém** |  |
| Bez interních disků |  |
| Samostatný diskový prostor pro boot operačního systému osazený NVMe hot-plug disky o kapacitě: min. kapacitě 480GB NVMe v RAID 1 |  |
| **Interface** |  |
| 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0  2 x VGA (1 vpředu, 1 vzadu) |  |
| **Rozhraní** |  |
| 2x Dual port karta 10/25GbE včetně optických transceiverů/DAC kabelů 25Gbit |  |
| 2x Dual port karta FC 32Gb včetně optických transceiverů a příslušných optických patchcordů |  |
| 1x Dual port 1GbE karta rozhraní RJ45 |  |
| 1x nezávislý management port s rozhraním RJ45 |  |
| **Napájení** |  |
| Plně redundantní napájecí zdroje min 1100W / max. 1600W min. třídy Titanium |  |
| **Management** |  |
| Samostatný management port s podporou failoveru na jinou síťovou kartu v serveru musí podporovat VLAN, LLDP Discovery síťové infrastruktury a protokoly IPv4 i IPv6 |  |
| Automatická instalace a obnova SSL certifikátu vestavěného serveru |  |
| Na čelní straně serveru umístěný displej, který zobrazuje základní údaje o serveru (min. IP adresu serveru a chybové stavy) |  |
| Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE |  |
| Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů, včetně událostí o přihlášení a změnách konfigurace |  |
| Možnost streamování údajů ze senzorů serveru, telemetrie a provozních reportů pro účely prediktivního vyhodnocování a zabezpečení, s podporou pro Splunk nebo ELK stack |  |
| Management musí být schopen poskytovat ovladače pro instalované operační systémy bez nutnosti speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS). Dále musí umožňovat aktualizaci firmware hardwaru s možností ověření a stažení aktuálních verzí z online repozitáře výrobce nebo z bezpečného lokálního repozitáře spravovaného administrátorem. |  |
| Možnost přístupu přes dedikovaný USB port s emulací síťového připojení |  |
| Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| Schopnost integrace do prostředí VMware vCenter a následná správa z tohoto prostředí, včetně diskového subsystému, bez nutnosti přihlašování se na rozhraní OOB. Management umožňuje monitorování spotřeby elektrické energie na úrovni serveru, hosta a virtuálního serveru (VMware) |  |
| Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, včetně vzdálené konzole KVM over IP, který zároveň umožňuje průběžné vyhodnocování průměrného vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů |  |
| Možnost vrácení firmware na předchozí verzi. Automatické obnovení zabezpečeného operačního systému včetně BIOSu serveru a firmware BMC. Podpora uzamčení serveru pro zvýšení bezpečnosti (System Lock Down) |  |
| Grafická konzole pro správu a monitorování serverů s možností integrace do proaktivního monitoringu s prediktivní analýzou prostřednictvím cloudového portálu výrobce. Tento portál je přístupný také přes mobilní aplikace dostupné pro iOS a Android. Pokud jsou vyžadovány licence, musí být součástí řešení po celou dobu platnosti podpory |  |
| **Podpora operační systémů a hypervizoru** |  |
| VMware vSphere™ 7.0 a novější  Microsoft® Windows Server® 2019/2022, x64  Microsoft® Windows Server® 2025, x64  SUSE® Linux® Enterprise Server  Ubuntu Server LTS  Red Hat® Enterprise Linux |  |
| **Záruka** |  |
| Podpora na 5 roků typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace, servis je poskytován výrobcem serveru. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla |  |
| Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |
| **Software** |  |
| Součástí dodávky je operační serverový systém s grafickým rozhraním v nejnovější verzi s autentizací protokoly Kerberos V5, NTLMv2, NTLM. S možností provozu neomezeného počet serverů v serverovém virtuálním prostředí pro všechna jádra každého serveru, dodávaná jako OEM přímo od výrobce serveru, licence musí být nová, nepoužitá a nesmí se jednat o druhotnou licenci. Dodávaný OS musí být plně kompatibilní se stávajícím operačními systémy, s používanou správou uživatelů (Active directory) a v současnosti provozované AIS na něm musí být schopny běžet bez nutnosti jejich změny. Součástí požadavku jsou také klientské licence v rozsahu 250 klientů plně kompatibilní s provozovanými OS. Součástí dodávky je technická dokumentace v elektronické podobě (případně odkaz na dokumentaci na stránkách výrobce). |  |
| Součástí dodávky je 250 ks Windows Server 2025 User CAL |  |
| Součástí dodávky je virtualizační platforma VMware v Sphere (z důvodů kompatibility se stávajícím prostředím a podporou a kompatibilitou provozovaných aplikací ze strany jejich výrobců). Součástí dodávky je VMware vSphere Standard pro všechna jádra v každém serveru na 5 let. |  |

**Disaster Recovery server 1 ks**

|  |  |
| --- | --- |
| **Server** | **Splněno ANO/NE** |
| Provedení do racku, barevně značené hot-plug vnitřní komponenty a místa pro uchopení |  |
| Výška max. 2U, šířka 19“, montáž do racku, výsuvné lyžiny včetně ramene pro kabely |  |
| Trusted Platform Module 2.0 |  |
| Dvousocketový systém založený na Intel platformě (z důvodu kompatibility se současným clusterem). |  |
| Osazený 2x CPU každý s přesně 16 fyzickými jádry (z licenčních důvodů na serverech provozovaných sysrémů) o základní frekvenci min. 2.8 GHz. Výkon CPU Throughput SPECrate® 2017 Integer minimálně 338 Base pro 2 socket sestavu. Tento výsledek testu musí být dostupný přímo pro nabízený konkrétní model konkrétního výrobce serveru. |  |
| Požadovaná kapacita RAM minimálně 1024 GB typu DDR5 5600MT/s složená z 16 dimm modulů. Musí umožnovat přidat min. dalších 1024 GB paměti ve stejných modulech a kapacitě, bez nutnosti výměny původních modulů. |  |
| **Diskový subsystém** |  |
| HW řadič s podporou HW RAID min. RAID 0, 1, 5, 6, 10, 50, 60 a min. 8GB zálohovanou cache na řadiči |  |
| Osazený právě 10x SSD (nebo NVME) o kapacitě jednoho disku min.3,84TB. Chassis musí umožňovat osazení dalších min. 6 ks stejných disků bez nutnosti dokupování jiných komponent než samotných disků. |  |
| Samostatný diskový prostor pro boot operačního systému osazený NVMe hot-plug disky o min. kapacitě 480GB NVMe v RAID 1 |  |
| **Interface** |  |
| 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0  2 x VGA (1 vpředu, 1 vzadu) |  |
| **Rozhraní** |  |
| 2x Dual port karta 10/25GbE včetně optických transceiverů/DAC kabelů 25Gbit |  |
| 2x Dual port karta FC 32Gb včetně optických transceiverů a příslušných optických patchcordů |  |
| 1x Dual port 1GbE karta rozhraní RJ45 |  |
| 1x nezávislý management port s rozhraním RJ45 |  |
| **Napájení** |  |
| Plně redundantní napájecí zdroje min 1100W / max. 1600W min. třídy Titanium |  |
| **Management** |  |
| Samostatný management port s podporou failoveru na jinou síťovou kartu v serveru musí podporovat VLAN, LLDP Discovery síťové infrastruktury a protokoly IPv4 i IPv6 |  |
| Automatická instalace a obnova SSL certifikátu vestavěného serveru |  |
| Na čelní straně serveru umístěný displej, který zobrazuje základní údaje o serveru (min. IP adresu serveru a chybové stavy) |  |
| Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE |  |
| Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů, včetně událostí o přihlášení a změnách konfigurace |  |
| Možnost streamování údajů ze senzorů serveru, telemetrie a provozních reportů pro účely prediktivního vyhodnocování a zabezpečení, s podporou pro Splunk nebo ELK stack |  |
| Management musí být schopen poskytovat ovladače pro instalované operační systémy bez nutnosti speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS). Dále musí umožňovat aktualizaci firmware hardwaru s možností ověření a stažení aktuálních verzí z online repozitáře výrobce nebo z bezpečného lokálního repozitáře spravovaného administrátorem. |  |
| Možnost přístupu přes dedikovaný USB port s emulací síťového připojení |  |
| Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| Schopnost integrace do prostředí VMware vCenter a následná správa z tohoto prostředí, včetně diskového subsystému, bez nutnosti přihlašování se na rozhraní OOB. Management umožňuje monitorování spotřeby elektrické energie na úrovni serveru, hosta a virtuálního serveru (VMware) |  |
| Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, včetně vzdálené konzole KVM over IP, který zároveň umožňuje průběžné vyhodnocování průměrného vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů |  |
| Možnost vrácení firmware na předchozí verzi. Automatické obnovení zabezpečeného operačního systému včetně BIOSu serveru a firmware BMC. Podpora uzamčení serveru pro zvýšení bezpečnosti (System Lock Down) |  |
| Grafická konzole pro správu a monitorování serverů s možností integrace do proaktivního monitoringu s prediktivní analýzou prostřednictvím cloudového portálu výrobce. Tento portál je přístupný také přes mobilní aplikace dostupné pro iOS a Android. Pokud jsou vyžadovány licence, musí být součástí řešení po celou dobu platnosti podpory |  |
| **Podpora operační systémů a hypervizoru** |  |
| VMware vSphere™ 7.0 a novější  Microsoft® Windows Server® 2019/2022, x64  Microsoft® Windows Server® 2025, x64  SUSE® Linux® Enterprise Server  Ubuntu Server LTS  Red Hat® Enterprise Linux |  |
| **Záruka** |  |
| Podpora na 5 roků typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace, servis je poskytován výrobcem serveru. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla |  |
| Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |
| **Software** |  |
| Součástí dodávky je operační serverový systém s grafickým rozhraním v nejnovější verzi s autentizací protokoly Kerberos V5, NTLMv2, NTLM. S možností provozu neomezeného počet serverů v serverovém virtuálním prostředí pro všechna jádra každého serveru, dodávaná jako OEM přímo od výrobce serveru, licence musí být nová, nepoužitá a nesmí se jednat o druhotnou licenci. Dodávaný OS musí být plně kompatibilní se stávajícím operačními systémy, s používanou správou uživatelů (Active directory) a v současnosti provozované AIS na něm musí být schopny běžet bez nutnosti jejich změny. Součástí požadavku jsou také klientské licence v rozsahu 250 klientů plně kompatibilní s provozovanými OS. Součástí dodávky je technická dokumentace v elektronické podobě (případně odkaz na dokumentaci na stránkách výrobce). |  |
| Součástí dodávky je z důvodů zalicencování DR prostředí pro běh stěžejní aplikace trvalá licence MS SQL v nejnovější verzi pro 4 core včetně Software Assurance platné na 3 roky od dodání. Licence musí být nová, nepoužitá a nesmí se jednat o druhotnou licenci. |  |
| Součástí dodávky je virtualizační platforma VMware vSphere (z důvodů kompatibility se stávajícím prostředím a podporou a kompatibilitou provozovaných aplikací ze strany jejich výrobců). Součástí dodávky je VMware vSphere Standard pro všechna jádra v serveru na 5 let. |  |

**Backup server 1 ks**

|  |  |
| --- | --- |
| **Server** | **Splněno ANO/NE** |
| Provedení do racku, barevně značené hot-plug vnitřní komponenty a místa pro uchopení |  |
| Výška max. 1U, šířka 19“, montáž do racku výsuvné lyžiny včetně ramene pro kabely |  |
| Dvousocketový systém založený na Intel platformě (z důvodu kompatibility se současným clusterem). |  |
| Trusted Platform Module 2.0 |  |
| Osazený 2x CPU každý s přesně 16 fyzickými jádry (z licenčních důvodů na serverech provozovaných sysrémů) o základní frekvenci min. 2 GHz. Výkon CPU Throughput SPECrate® 2017 Integer minimálně 265 Base pro 2 socket sestavu. Tento výsledek testu musí být dostupný přímo pro nabízený konkrétní model konkrétního výrobce serveru. |  |
| Požadovaná kapacita RAM minimálně 256 GB typu DDR5 5600MT/s složená z 16 dimm modulů. Musí umožnovat přidat min. dalších 256 GB paměti ve stejných modulech a kapacitě, bez nutnosti výměny původních modulů. |  |
| **Diskový subsystém** |  |
| HW řadič s podporou HW RAID min. RAID 0, 1, 5, 6, 10, 50, 60 a min. 8GB zálohovanou cache na řadiči |  |
| Osazený min. 3x SSD (nebo NVME) o kapacitě jednoho disku min.960GB. Chassis musí umožňovat osazení dalších min. 5 ks stejných disků bez nutnosti dokupování jiných komponent než samotných disků. |  |
| **Interface** |  |
| 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0  2 x VGA (1 vpředu, 1 vzadu) |  |
| **Rozhraní** |  |
| 2x Dual port karta 10/25GbE včetně optických transceiverů/DAC kabelů 25Gbit |  |
| 1x Dual port karta FC 32Gb včetně optických transceiverů a příslušných optických patchcordů |  |
| 1x Dual port 1GbE karta rozhraní RJ45 |  |
| 1x nezávislý management port s rozhraním RJ45 |  |
| **Napájení** |  |
| Plně redundantní napájecí zdroje min 1100W / max. 1600W min. třídy Titanium |  |
| **Management** |  |
| Samostatný management port s podporou failoveru na jinou síťovou kartu v serveru musí podporovat VLAN, LLDP Discovery síťové infrastruktury a protokoly IPv4 i IPv6 |  |
| Automatická instalace a obnova SSL certifikátu vestavěného serveru |  |
| Na čelní straně serveru umístěný displej, který zobrazuje základní údaje o serveru (min. IP adresu serveru a chybové stavy) |  |
| Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE |  |
| Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů, včetně událostí o přihlášení a změnách konfigurace |  |
| Možnost streamování údajů ze senzorů serveru, telemetrie a provozních reportů pro účely prediktivního vyhodnocování a zabezpečení, s podporou pro Splunk nebo ELK stack |  |
| Management musí být schopen poskytovat ovladače pro instalované operační systémy bez nutnosti speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS). Dále musí umožňovat aktualizaci firmware hardwaru s možností ověření a stažení aktuálních verzí z online repozitáře výrobce nebo z bezpečného lokálního repozitáře spravovaného administrátorem. |  |
| Možnost přístupu přes dedikovaný USB port s emulací síťového připojení |  |
| Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| Schopnost integrace do prostředí VMware vCenter a následná správa z tohoto prostředí, včetně diskového subsystému, bez nutnosti přihlašování se na rozhraní OOB. Management umožňuje monitorování spotřeby elektrické energie na úrovni serveru, hosta a virtuálního serveru (VMware) |  |
| Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, včetně vzdálené konzole KVM over IP, který zároveň umožňuje průběžné vyhodnocování průměrného vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů |  |
| Možnost vrácení firmware na předchozí verzi. Automatické obnovení zabezpečeného operačního systému včetně BIOSu serveru a firmware BMC. Podpora uzamčení serveru pro zvýšení bezpečnosti (System Lock Down) |  |
| Grafická konzole pro správu a monitorování serverů s možností integrace do proaktivního monitoringu s prediktivní analýzou prostřednictvím cloudového portálu výrobce. Tento portál je přístupný také přes mobilní aplikace dostupné pro iOS a Android. Pokud jsou vyžadovány licence, musí být součástí řešení po celou dobu platnosti podpory |  |
| **Podpora operační systémů a hypervizoru** |  |
| VMware vSphere™ 7.0 a novější  Microsoft® Windows Server® 2019/2022, x64  Microsoft® Windows Server® 2025, x64  SUSE® Linux® Enterprise Server  Ubuntu Server LTS  Red Hat® Enterprise Linux |  |
| **Záruka** |  |
| Podpora na 5 roků typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace, servis je poskytován výrobcem serveru. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla |  |
| Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |
| **Software** |  |
| Součástí dodávky je operační serverový systém s grafickým rozhraním v nejnovější verzi s autentizací protokoly Kerberos V5, NTLMv2, NTLM. S možností provozu 2 serverů v serverovém virtuálním prostředí pro všechna jádra každého serveru, dodávaná jako OEM přímo od výrobce serveru, licence musí být nová, nepoužitá a nesmí se jednat o druhotnou licenci. Dodávaný OS musí být plně kompatibilní se stávajícím operačními systémy, s používanou správou uživatelů (Active directory) a v současnosti provozované AIS na něm musí být schopny běžet bez nutnosti jejich změny. Součástí požadavku jsou také klientské licence v rozsahu 250 klientů plně kompatibilní s provozovanými OS. Součástí dodávky je technická dokumentace v elektronické podobě (případně odkaz na dokumentaci na stránkách výrobce). |  |
| Součástí dodávky je z důvodů zachování provozu a kompatibility licence zálohovacího software Veeam Essentials VUL pro 50 instancí na 5 let |  |

|  |  |  |
| --- | --- | --- |
| **Požadovaný parametr** | **Splňuje**  **ANO/NE** | **Popis řešení požadavku/**  **skutečná hodnota** |
| **Deduplikační diskové úložiště – 1 ks** | | |
| Výrobce a obchodní název nabízeného zařízení |  | |
| Deduplikační diskové úložiště, provedení RACK – šíře 19” |  |  |
| Čistá využitelná kapacita (nededuplikovaná kapacita, která je dostupná pro uložení dat a lze ji zkontrolovat prostřednictvím management nástrojů): min. 92TBu |  |  |
| Možnost rozšíření kapacity minimálně až na 172TBu čisté kapacity. |  |  |
| Propustnost pro zápis: min. 21TB/h |  |  |
| Propustnost pro čtení: min. 3TB/h |  |  |
| Síťové rozhraní 10GbE SFP: počet rozhraní min. 4x, včetně 4x 10GbE 3m AOC kabelů |  |  |
| FC16Gb: minimální počet portů 2x, osazeno FC moduly |  |  |
| Možnost rozšíření:  • FC16 (min. 2 porty)  • 25GbE (min. 2x SFP+ porty)  • 10GbE (min. 4x SFP+ porty) |  |  |
| Minimální počet konkurenčních zálohovacích úloh: min. 260 |  |  |
| Úložiště musí při ukládání dat využívat princip in-line deduplikace na cíli na principu variabilní délky bloku. |  |  |
| Úložiště musí data před uložením komprimovat (komprimace nesmí mít dopad na výkon úložiště při záloze nebo obnově dat) |  |  |
| Architektura diskového úložiště musí pro deduplikace využívat procesorový výkon a nesmí být závislá na počtu a typu backendových disků |  |  |
| Diskové úložiště musí konsolidovat a centralizovat zálohovací prostředí (lokální i vzdálené) – všechna data budou deduplikována v rámci jednoho boxu |  |  |
| Zařízení musí podporovat minimálně vyjmenované protokoly a musí umožnit jejich současné použití: CIFS, NFS, VTL, FC |  |  |
| Zařízení musí umožňovat přímou integraci s různými typy zálohovacích SW (minimálně Microfocus Data Protector, Veritas NetBackup, Avamar, PPDM, Veeam, Oracle RMAN, MS SQL Studio) |  |  |
| Diskové úložiště musí umožňovat přímou integraci se zálohovacím software - Veeam Backup Veeam Backup & Replication v12. Přímá integrace musí být doložitelná jak výrobcem diskového úložiště, tak výrobcem software, tzn. společností Veeam na veřejně dostupném místě (např. <https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120>)  Popište způsob integrace |  |  |
| Diskové úložiště je univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí – tzn. soubory, databáze, emaily, VMware, MS Exchange |  |  |
| Kompatibilita se standardem OpenStorage |  |  |
| Požadujeme Certifikace podle SEC 17a-4f nebo ekvivalentní evropské nebo české normy, uchazeč uvede jednotlivé certifikace. |  |  |
| Deduplikace je prováděna přes celé zálohovací prostředí – jak přes všechny aplikace, tak přes cílová úložiště |  |  |
| Možnost distribuce deduplikačního algoritmu z cílového (deduplikačního úložiště) na zdrojové zařízení (backup klienta nebo backup server) |  |  |
| Funkce multitenancy (logické dělení diskového prostoru pro různé skupiny uživatelů s právy pouze na tyto logické jednotky s možností definice tenant administrator) |  |  |
| Diskové úložiště musí obsahovat licenci pro replikaci do záložní lokality |  |  |
| Diskové úložiště musí posílat do záložní lokality pouze deduplikovaná zkomprimovaná data |  |  |
| Diskové úložiště musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci |  |  |
| Replikaci musí být možno spustit ve stejném čase jako zálohu bez dopadu na výkon zálohy |  |  |
| Diskové úložiště musí umožnit funkcionalitu šifrování replikačního toku data-in-flight |  |  |
| Interní algoritmus pro neustálou kontrolu zdraví uložených dat a jejich automatickou obnovu v případě poškození tak, aby bylo možno zálohy kdykoliv obnovit k jakémukoliv okamžiku |  |  |
| Zařízení musí obnovovat data vždy z deduplikovaného a komprimovaného stavu, není přípustný mezikrok (např. externí disková cache), |  |  |
| Funkcionalita pro šifrování ukládaných data metodou data-at-rest |  |  |
| Úložiště musí obsahovat HotSpare disky |  |  |
| Kompletní verifikace dat – okamžitá verifikace záloh a kontrola integrity právě ukládaných dat |  |  |
| Úložiště musí disponovat mechanismem pro mazání expirovaných dat, který nebude mít dopad na úlohy zálohy, obnovy a replikace (nebude snižovat počty současně běžících úloh, nebude vynucovat maintenance window, atd.) – tento proces musí být možno v případě potřeby spustit, nebo přerušit bez jakéhokoliv dopadu na zdraví a konzistenci uložených dat |  |  |
| Nabízené zařízení musí umožňovat šifrovat data a musí disponovat i nástroji pro správu klíčů. |  |  |
| Úložiště musí umožňovat nastavit skartační lhůty uložených dat, granulárně podle definovaných politik řízených zálohovacím SW. |  |  |
| Retenční zámek úložiště musí ochránit data před změnou, nebo smazáním před vypršením retenční lhůty |  |  |
| Úložiště musí disponovat mechanismem ochrany dat a samotného úložiště před napadením útočníkem z prostředí zadavatele i mimo toto prostředí (např. hackerský útok, ransomware, apod.). |  |  |
| Úložiště musí umožnit tzv. HW hardening – tedy takové nastavení, aby nebylo možno jedním uživatelem s dostatečnými právy manipulovat s uloženými daty nebo systémovým nastavením (např. princip čtyř očí). Požadujeme aby bylo možné data ošetřit tak, aby neexistovala oprávněná osoba, či soubor osob, které by je mohly modifikovat či smazat. |  |  |
| Správa prostřednictvím jednotného webového rozhraní |  |  |
| Funkcionalita automatického reportingu, automatický call-home (tato funkce musí mít možnost deaktivace na přání zadavatele) |  |  |
| Monitoring pomocí MP pro SCOM aktuální verze |  |  |
| Správu na principu rolí s různými typy oprávnění |  |  |
| Záruka a podpora výrobce na 5 let s reakční dobou NBD (Next Business Day), 24x7 pro chybu, která znemožňuje chod systému nebo má dopad na fungování systému. Přístup k telefonické podpoře výrobce 24x7x365. Aktualizace systému dostupné min. po dobu záruky zdarma, nabízené v servisním portálu výrobce po zadání sériového čísla. |  |  |
| Možnost sledování servisních reportů prostřednictvím internetu. |  |  |
| Instalace a konfigurace do stávajícího prostředí |  |  |
| **Rozšíření stávajícího diskového úložiště – 1 ks** | | |
| Rozšíření stávajícího diskového pole IBM FlashSystem 5300 o 6ks nových nepoužitých 19,2 TB FCM 4 disků se zárukou 5 YEAR IBM STORAGE EXPERT CARE ADVANCED 24HR COMMITTED FIX. Z důvodů kompatibility celého řešení musí být dodržen přesný typ disků i záruky. |  |  |
| Instalace a konfigurace do stávajícího diskového pole |  |  |

**Specifikace FC switche 2 kusy**

|  |  |
| --- | --- |
| **FC switche každý** | **Splněno ANO/NE** |
| Provedení do racku s chlazením Rear to front (výdech dozadu na porty) |  |
| Výška max. 1U, šířka 19“, příslušenství pro montáž do racku |  |
| Architektura kompatibilní s Brocade Fabric |  |
| Kompatibilita s DS-6610B-L a Brocade 6505 |  |
| **Rozhraní** |  |
| SAN switch musí být vybaven minimálně 24 porty |  |
| SAN switch musí mít minimálně 24 plně licencovaných/aktivovaných a osazených portů. Osazený port bude mít přenosovou rychlost 32Gbps SFP+ a bude osazen originálním SW SFP+ modulem, alternativní SFP+ jsou nepřípustné |  |
| Možnost osazení jakéhokoli portu nabízených SAN switchů modulem o rychlosti 32 GBps SFP+ a 16 GBps SFP+ |  |
| Podpora auto-sensing na switchi 8, 16, 32 GBps port rychlost |  |
| 1x RJ45 ethernet pro vzdálenou správu |  |
| **Management** |  |
| Informace o stavu zařízení je možno sledovat minimálně pomocí protokolu SNMP v. 3 |  |
| Podpora Advanced Web Tools; Command Line Interface (CLI) |  |
| Obsahuje licence Fabric Vision, Extended Fabric a ISL Trunking |  |
| **Další požadavky** |  |
| Požadavek kybernetické bezpečnosti, SAN switche ani jejich výrobce nesmí být uvedeny ve Varování Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). |  |
| **Záruka** |  |
| Podpora na 5 let typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace, servis je poskytován výrobcem. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla |  |
| Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |

1. Doplní účastník [↑](#footnote-ref-1)
2. Doplní účastník [↑](#footnote-ref-2)
3. Níže v textu je kupující označen rovněž jako „zadavatel“ a prodávající jako „dodavatel“. [↑](#footnote-ref-3)