KUMSP00U42E9

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

MORAVSKOSLEZSKÝ KRAJ - KRAJSKÝ ÚŘAD

ČÍSLO SMLOUVY (DODATKU) -4-		
04029	2018	TMS
poř. číslo	rok	zkr. odb.

SMLOUVA O DÍLO

I.
Smluvní strany

1. **Moravskoslezský kraj**
   se sídlem: 28. října 117, 702 18 Ostrava
   zastoupen: prof. Ing. Ivo Vondrákem, CSc., hejtmanem kraje
   IČO: 70890692
   DIČ: CZ70890692
   bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.
   číslo účtu: 2105987779/2700

   Osoby oprávněné jednat ve věcech smlouvy:

   [redacted]

   Osoba oprávněná jednat ve věcech realizace projektu a řízení projektu:

   [redacted]

   (dále jen „objednatel")

2. **VÍTKOVICE IT SOLUTIONS a.s.**
   se sídlem: Cihelní 1575/14, 702 00 Ostrava-Moravská Ostrava
   zastoupena: Ing. Vladimírem Měkotou, místopředsedou představenstva
   Ing. Milanem Juříkem, členem představenstva

   IČO: 28606582
   DIČ: CZ28606582
   bankovní spojení: Česká spořitelna, a.s.
   číslo účtu: 4312807389/0800

   Zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě, oddíl B, vložka 4229

   (dále jen „zhotovitel")

II.
Základní ustanovení

1. Tato smlouva je uzavřena dle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník"); práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku.

[redacted]

2. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu se skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
3. Je-li zhotovitel plátcem DPH, prohlašuje, že bankovní účet uvedený v čl. I odst. 2 této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH"). V případě změny účtu zhotovitele je zhotovitel povinen doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu; je-li zhotovitel plátcem DPH, musí být nový účet zveřejněným účtem ve smyslu předchozí věty.
4. Předmět této smlouvy bude spolufinancován z Evropského fondu pro regionální rozvoj (dále jen „EFRR"), v rámci projektu „„**Modernizace výuky svařování**", registrační číslo projektu: CZ.06.2.67/0.0/0.0/16_050/0002605, předkládaného do Integrovaného regionálního operačního programu (dále jen „IROP") po období 2014 – 2020, výzva č. 33 INFRASTRUKTURA STŘEDNÍCH ŠKOL A VYŠŠÍCH ODBORNÝCH ŠKOL (dále také „výzva"), pro specifický cíl 2.4 „Zvýšení kvality a dostupnosti infrastruktury pro vzdělávání a celoživotní učení" (dále jen „projekt"). Zhotovitel bere na vědomí, že předmětem smlouvy jsou aktivity a výstupy, které budou tvořit součást projektu spolufinancovaného Evropskou unií v rámci IROP.
5. Smluvní strany se zavazují postupovat v souladu s Programovým dokumentem IROP a Obecnými pravidly pro žadatele a příjemce IROP, v souladu s výzvou, specifickými pravidly pro žadatele a příjemce IROP relevantní pro účel a předmět této smlouvy a v souladu s oficiálními doporučeními a oznámeními řídícího orgánu či zprostředkujícího subjektu dané výzvy v aktuálním platném znění.
6. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.
7. Smluvní strany prohlašují, že předmět plnění smlouvy není plněním nemožným a že smlouvu uzavírají po pečlivém zvážení všech možných důsledků.
8. Zhotovitel potvrzuje, že se detailně seznámil s rozsahem a povahou díla, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci díla a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci díla za dohodnutou smluvní cenu uvedenou v čl. IV odst. 1 této smlouvy.
9. Účelem této smlouvy je naplnění standardu konektivity dle IROP na Střední škole, Havířov-Šumbark, Sýkorova 1/613, příspěvkové organizaci (dále jen „SŠ Havířov", případně „uživatel").

III.
Předmět smlouvy

1. Předmětem této smlouvy je pořízení a implementace vybavení zajišťujícího kvalitní a bezpečný síťový provoz (WAN, LAN) včetně vypracování potřebné dokumentace v češtině a zajištění provozu.
2. Zhotovitel se zavazuje provést na SŠ Havířov na svůj náklad a nebezpečí pro objednatele dílo v rozsahu a kvalitě dle této smlouvy, zejm. dle přílohy č. 1 této smlouvy (dále jen „dílo").
3. Součástí díla jsou veškeré práce a služby nezbytné pro řádné a úplné zprovoznění díla, včetně vytvoření dokumentací a postupů pro správce a uživatele ke všem technickým částem díla.
4. Dílo je tvořeno těmito částmi realizovanými ve dvou fázích:
   4.1. I. fáze - realizační a implementační (včetně dokumentace a zaškolení obsluhy)
   4.2. II. fáze - provozní (technická podpora, aktualizace, servis)
5. Objednatel se zavazuje řádně a včas provedené dílo převzít a uhradit za ně zhotoviteli sjednanou cenu dle čl. IV odst. 1 této smlouvy. Objednatel je dále povinen hradit zhotoviteli sjednanou cenu za poskytovanou servisní a technickou podporu.

IV.
Cena za dílo

1. Cena v Kč za dílo činí:

	Cena bez DPH	DPH ve výši 21 %	Cena včetně DPH
Cena za dílo celkem	2 000 122,- Kč	420 025,62 Kč	2 420 147,62 Kč
Cena za I. fázi - realizační a implementační	1 377 595,- Kč	289 294,95 Kč	1 666 889,95 Kč
Cena za II. fázi – provozní (celkem za 5 let)	622 527,- Kč	130 730,67 Kč	753 257,67 Kč
Z toho cena za II. fázi za 1 rok – 20 %	124 505,40 Kč	26 146,13 Kč	150 651,53 Kč

Podrobný rozpis ceny za dílo je přílohou č. 4 této smlouvy.

2. Cena za dílo podle odst. 1 tohoto článku smlouvy zahrnuje veškeré náklady zhotovitele spojené se splněním jeho závazků vyplývajících z této smlouvy, tj. cenu díla včetně poskytování servisní a technické podpory, dopravného, odměny za poskytnutí licence, práce technika apod. Cena za dílo je stanovena jako nejvýše přípustná a není ji možno překročit.
3. Je-li zhotovitel plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, je zhotovitel k ceně díla bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny díla v důsledku změny sazby DPH není nutno ke smlouvě uzavírat dodatek. V případě, že zhotovitel stanoví sazbu DPH či DPH v rozporu s platnými právními předpisy, je povinen uhradit objednateli veškerou škodu, která mu v souvislosti s tím vznikla.
4. Zhotovitel sestaví podrobný rozpis ceny předmětu plnění (bez DPH) za účelem evidence majetku a odepisování dle zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, kde bude uvedena i klasifikace dle kódů CZ-CPA a CZ-CC. Tento rozpis bude objednateli předán zhotovitelem do 2 měsíců ode dne, kdy tato smlouva nabude účinnosti.

V.
Doba a místo plnění, předání díla, předávací protokol, převod vlastnického práva a nebezpečí škody na díle

1. Zhotovitel je povinen provést dílo (resp. I. fázi realizační a implementační) **do 14 týdnů** od nabytí účinnosti této smlouvy. Poslední 2 týdny jsou určeny pouze pro připomínkování dokumentace, zaškolení a testování.
2. Zhotovitel je povinen předat objednateli dílo v místě plnění, kterým je Střední škola, Havířov-Šumbark, Sýkorova 1/613, příspěvková organizace.
3. Zhotovitel je povinen do 7 dnů od nabytí účinnosti smlouvy předložit objednateli ke schválení **detailní realizační návrh**, jehož součástí bude **návrh akceptačních testů** a **podrobný harmonogram** realizace díla se specifikovanými požadavky na součinnost objednatele, resp. uživatele. Tento bod nemá vliv na dobu plnění dle odst. 1 tohoto článku smlouvy.

4. V rámci II. fáze - **provozní fáze** (technická podpora, aktualizace, servis) bude zhotovitelem poskytována servisní a technická podpora **po dobu 5 let** od převzetí díla bez vad a nedodělků dle čl. V odst. 5 této smlouvy, a to v rozsahu dle přílohy č. 2 smlouvy.
5. Dílo je provedeno, je-li dokončena realizační a implementační fáze. Smluvní strany se dohodly, že **objednatel není povinen dílo převzít, pokud toto vykazuje vady či nedodělky**. Smluvní strany prohlašují, že jednotlivé součásti díla se samostatně nepřebírají, neboť plnění jednotlivých částí samostatně nemá pro objednatele význam a teprve provedením všech částí je možné ověřit funkčnost díla.
6. Objednatel se zavazuje dílo převzít v případě, že bude předáno bez vad a nedodělků. O předání a převzetí díla zhotovitel sepíše předávací protokol, ve kterém objednatel prohlásí, zda dílo přejímá či nikoli.
7. Pokud objednatel dílo nepřevezme, protože obsahuje vady či nedodělky, potvrdí tuto skutečnost v předávacím protokolu předloženém zhotovitelem. Objednatel je dále povinen tyto vady či nedodělky specifikovat a tuto specifikaci předat zhotoviteli. Specifikace vad a nedodělků díla vyhotovená objednatelem se tímto stane přílohou a nedílnou součástí předávacího protokolu vyhotoveného zhotovitelem. K vypracování specifikace vad a nedodělků je zhotovitel povinen poskytnout objednateli součinnost.
8. Předávací protokol musí obsahovat minimálně tyto náležitosti:
   a) číslo předávacího protokolu a datum jeho vyhotovení, místo vyhotovení,
   b) číslo této smlouvy a datum jejího uzavření (vč. data účinnosti smlouvy), číslo veřejné zakázky,
   c) označení předmětu plnění, tj. text „Naplnění standardu konektivity dle IROP na SŠ Havířov",
   d) označení objednatele a zhotovitele,
   e) text ve znění: Projekt „Modernizace výuky svařování", reg. č. CZ.06.2.67/0.0/0.0/16_050/0002605 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného regionálního operačního programu",
   f) prohlášení objednatele, že dílo přejímá či nikoliv a prohlášení zhotovitele, že předané dílo je bez vad a nedodělků a plně funkční; pokud dílo nebude objednatelem převzato, bude protokol obsahovat jako svou přílohu specifikaci vad díla dle předchozího odstavce této smlouvy,
   g) jména a podpisy zástupců objednatele a zhotovitele; kontaktní telefon a e-mail zástupce zhotovitele odpovědného za vyhotovení předávacího protokolu.
9. Předávací protokol bude doručen doporučeně prostřednictvím provozovatele poštovních služeb, datovou schránkou nebo osobně pověřenému zaměstnanci objednatele proti písemnému potvrzení.
10. Vlastnické právo k dílu, případně k věci, která je předmětem díla a nebezpečí škody na ní přechází na objednatele dnem převzetí díla objednatelem.

VI.
Práva a povinnosti smluvních stran

1. Není-li stanoveno touto smlouvou výslovně jinak, řídí se vzájemná práva a povinnosti smluvních stran ustanoveními § 2586 a následujícími občanského zákoníku.
2. Zhotovitel je zejména povinen:
   a) Provést dílo řádně a včas za použití materiálu a postupů odpovídajících právním předpisům a technickým normám ČR. Smluvní strany se dohodly na I. jakosti díla. Dílo musí odpovídat příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k provedení díla a umožňovat užívání, k němuž bylo určeno a zhotoveno.
   b) Řídit se při provádění díla pokyny objednatele, i prostřednictvím uživatele.
   c) Umožnit objednateli kontrolu provádění díla, a to kdykoliv po dobu provádění díla. Pokud objednatel zjistí, že zhotovitel neprovádí dílo řádně či jinak porušuje svou povinnost, poskytne zhotoviteli lhůtu k nápravě; neučiní-li tak zhotovitel ve stanovené lhůtě, je objednatel oprávněn od smlouvy odstoupit.

d) Odstranit zjištěné vady a nedodělky na své náklady.

e) Dbát při provádění díla dle této smlouvy na ochranu životního prostředí a dodržovat platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí.

f) Postupovat při provádění díla s odbornou péčí.

3. Objednatel i uživatel je povinen poskytnout zhotoviteli součinnost nutnou k provedení díla.

4. Zjistí-li zhotovitel při plnění předmětu smlouvy skryté překážky bránící řádnému provedení předmětu plnění, je povinen to bez odkladu **oznámit** objednateli a navrhnout další postup.

5. Zhotovitel se zavazuje práce v SŠ Havířov vykonávat **po dohodě a v koordinaci** s provozem uživatele.

6. Zhotovitel je povinen písemně informovat objednatele o všech svých **poddodavatelích** (včetně jejich identifikačních a kontaktních údajů a o tom, které služby a činnosti pro něj v rámci předmětu plnění této smlouvy každý z poddodavatelů poskytuje) a o případné změně poddodavatele, a to nejpozději do 7 kalendářních dnů ode dne, kdy zhotovitel uzavřel s poddodavatelem smlouvu upravující takovou poddodávku či ode dne, kdy došlo ke změně poddodavatele. Zhotovitel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení, jen z vážných důvodů a s předchozím písemným souhlasem objednatele, přičemž nový poddodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, kterým původní poddodavatel prokázal splnění kvalifikace za zhotovitele.

7. Zhotovitel je povinen průběžně objednatele **informovat o průběhu prací**. V rámci kontrolních oprávnění objednatele dle odst. 2 písm. c) tohoto článku se budou konat pravidelné **kontrolní dny** v místě plnění, které budou probíhat ode dne nabytí účinnosti smlouvy, a to v následujících intervalech:

   - v průběhu I. fáze (realizační a implementační) dvakrát měsíčně;
   - objednatel může dle aktuální potřeby frekvenci konání těchto kontrolních dní snížit nebo zvýšit, a to dle rozhodnutí objednatele.

   Kontrolních dní se musí zúčastnit vždy minimálně jeden kompetentní a odpovědný člen realizačního týmu zhotovitele.

8. Zhotovitel je povinen z každého jednání a z každého kontrolního dne týkajícího se plnění předmětu smlouvy bezprostředně po jeho skončení vyhotovit **zápis o průběhu a závěrech** jednání či kontrolního dne, který bude v případě odsouhlasení podepsán zástupci objednatele i zhotovitele, a to bezprostředně po jednání (nejpozději do pěti pracovních dnů) a současně odeslán na e-mail objednatele nebo bude objednateli předán jinou obdobnou formou. Každý ze zápisů bude obsahovat minimálně tyto náležitosti: pořadové číslo zápisu, datum konání, místo konání, seznam přítomných či omluvených účastníků, program jednání, popis sjednaných úkolů a závěrů jednání či kontrolního dne; popis splnění úkolů ujednaných na předchozím jednání či předchozím kontrolním dni.

9. Zhotovitel je dále povinen bez zbytečného odkladu oznámit objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky provádění díla. Zejména je povinen neprodleně písemně oznámit objednateli jakoukoliv změnu svých identifikačních údajů a změny své majetkoprávní struktury, jako je např. přeměna či fúze společnosti, snížení základního kapitálu, vstup do likvidace, vyhlášení úpadku či prohlášení konkurzu apod.

10. Zhotovitel je povinen dodržovat bezpečnostní požadavky, které jsou zejména obsaženy v bezpečnostních zásadách a zásadách zabezpečení dat uživatele. Tyto zásady budou zhotoviteli na vyžádání poskytnuty.

11. Zhotovitel je povinen **uchovávat** veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do konce roku 2028. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji zhotovitel použít.

12. Zhotovitel je povinen minimálně do konce roku 2028 **poskytovat požadované informace** a dokumentaci související s realizací projektu 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.

VII.
Platební a fakturační podmínky

1. Úhrada ceny za dílo bude provedena jednorázově po provedení díla v I. fázi (tj. po provedení realizační a implementační fáze dle čl. V odst. 1 této smlouvy) ve výši dle čl. IV odst. 1 této smlouvy. Zálohové platby nebudou poskytovány.
2. Úhrada ceny II. fáze - provozní fáze (technická podpora, aktualizace, servis) ve výši ceny uvedené v řádku „Z toho cena za II. fázi za 1 rok – 20 %" dle čl. IV odst. 1 této smlouvy bude prováděna vždy zpětně za období posledních 12 měsíců, po které byla poskytována.

   Podkladem pro prokázání poskytnutí technické podpory, aktualizace, servisu v II. fázi bude Soupis provedených prací za daný rok podepsaný uživatelem. Na přesné podobě Soupisu se smluvní strany dohodnou před fakturací.
3. **Je-li zhotovitel plátcem DPH**, podkladem pro úhradu ceny za dílo budou faktury, které budou mít náležitosti daňového dokladu dle zákona o DPH a náležitosti stanovené dalšími obecně závaznými právními předpisy. **Není-li zhotovitel plátcem DPH**, podkladem pro úhradu ceny za dílo budou faktury, které budou mít náležitosti účetního dokladu dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a náležitosti stanovené dalšími obecně závaznými právními předpisy.

   Faktury musí dále obsahovat:

   a) číslo smlouvy objednatele, číslo veřejné zakázky (tj. 220/2017), IČO objednatele,

   b) text ve znění: Projekt „Modernizace výuky svařování", reg. č. CZ.06.2.67/0.0/0.0/16_050/0002605je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného regionálního operačního programu",

   c) předmět smlouvy, tj. text: „pořízení a implementace vybavení zajišťujícího kvalitní a bezpečný síťový provoz (WAN, LAN) včetně vypracování potřebné dokumentace a zajištění provozu",

   d) označení banky a číslo účtu, na který musí být zaplaceno (pokud je číslo účtu odlišné od čísla uvedeného v čl. I odst. 2, je zhotovitel povinen o této skutečnosti v souladu s čl. II odst. 2 této smlouvy informovat objednatele),

   e) lhůtu splatnosti faktury,

   f) označení osoby, která fakturu vyhotovila, včetně jejího podpisu, kontaktního telefonu a e-mailu,

   g) označení útvaru objednatele, který případ likviduje (odbor evropských projektů po dobu I. fáze, poté odbor školství, mládeže a sportu po dobu II. fáze),

   h) Přílohou faktury bude předávací protokol (kopie). Ve II. fázi bude přílohou faktur Soupis provedených prací za daný rok.

   i) Přílohou faktury bude podrobný rozpis ceny předmětu plnění za účelem evidence majetku a jeho odepisování dle zákona č. 586/1992 Sb., o daních z příjmu, ve znění pozdějších předpisů a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. U dlouhodobého hmotného a nehmotného majetku bude uveden klasifikační kód CZ-CPA za účelem odepisování dlouhodobého hmotného a nehmotného majetku.
4. Povinnost zaplatit cenu za dílo je splněna dnem odepsání příslušné částky z účtu objednatele.
5. Lhůta splatnosti faktury činí s ohledem na povahu závazku 30 kalendářních dnů ode dne jejího doručení objednateli. Doručení faktury se provede osobně oproti podpisu zmocněné osoby objednatele nebo doručenkou prostřednictvím provozovatele poštovních služeb.

6. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy s vyznačením důvodu vrácení. Zhotovitel provede opravu vystavením nové faktury. Vrácením vadné faktury zhotoviteli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne doručení nové faktury objednateli.
7. Objednatel, příjemce plnění, prohlašuje, že plnění, které je předmětem smlouvy, nepoužije pro svou ekonomickou činnost, ale výlučně pro účely související s jeho činností při výkonu veřejné správy, při níž se nepovažuje za osobu povinnou k dani (viz § 5 odst. 3 zákona o DPH). Z uvedeného důvodu se na plnění, podléhá-li režimu přenesení daňové povinnosti dle příslušných ustanovení uvedeného zákona, tento daňový režim nevztahuje a zhotovitelem, je-li plátcem DPH, bude vystavena faktura za zdanitelné plnění včetně daně z přidané hodnoty.
8. Je-li zhotovitel plátcem DPH, objednatel uplatní institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uhradí v termínu splatnosti faktury stanoveném dle smlouvy přímo na osobní depozitní účet zhotovitele vedený u místně příslušného správce daně v případě, že:
   a) zhotovitel bude ke dni poskytnutí úhrady nebo ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr DPH" jako nespolehlivý plátce, nebo
   b) zhotovitel bude ke dni poskytnutí úhrady nebo ke dni uskutečnění zdanitelného plnění v insolvenčním řízení, nebo
   c) bankovní účet zhotovitele určený k úhradě plnění uvedený na faktuře nebude správcem daně zveřejněn v aplikaci „Registr DPH".

   Tato úhrada bude považována za splnění části závazku odpovídající příslušné výši DPH sjednané jako součást smluvní ceny za předmětné plnění. Objednatel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně zhotoviteli v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně.

VIII.
Licence a podmínky užití díla

1. Objednatel je oprávněn dílo užít ve smyslu ustanovení § 2371 a násl. občanského zákoníku (dále též „licence"), a to:
   - v původní nebo zpracované či jinak změněné podobě,
   - bez časového a územního omezení,
   - všemi způsoby užití.

   Odměna zhotovitele, coby autora díla, za poskytnutí licence je součástí ceny za dílo podle čl. IV této smlouvy.
2. Zhotovitel poskytuje touto smlouvou objednateli a objednatel touto smlouvou přijímá nevýhradní oprávnění k užití díla, včetně jeho aktualizací zejména podle vývoje relevantní právní úpravy, a to v rozsahu nezbytném pro řádné užívání díla objednatelem a jím určenými osobami. Objednatel může oprávnění tvořící součást licence poskytnout zcela nebo zčásti třetím subjektům (podlicence).
3. Zhotovitel musí zajistit licence ke všem SW technologiím zajišťujícím plnohodnotný provoz díla se všemi provozuschopnými funkcionalitami.
4. Není-li dále výslovně stanoveno jinak, územní a časový rozsah veškerých licencí dle této smlouvy je neomezený, licence jsou neodvolatelné a objednatel (či další oprávněné osoby) nejsou povinni licence využít.
5. Pokud není ve smlouvě uvedeno jinak, tak počet uživatelů díla není omezen, proto musí zhotovitel v případě potřeby zajistit multilicence pro neomezený počet uživatelů ke všem dodaným SW technologiím, u kterých je to nezbytné pro dostupnost díla dle této smlouvy pro neomezený počet koncových uživatelů.

6. Objednatel má právo realizovat rozhraní díla s jinými, jím provozovanými softwarovými produkty.
7. Dojde-li v rámci plnění předmětu smlouvy k pořízení databáze, pak je objednatel od okamžiku pořízení databáze oprávněn databázi užívat; objednatel má v tom případě postavení pořizovatele databáze dle § 89 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon").
8. Zhotovitel výslovně prohlašuje, že je plně oprávněn disponovat právy k duševnímu vlastnictví, včetně práv autorských zahrnutých v předmětu plnění dle této smlouvy, a zavazuje se za tímto účelem zajistit řádné a nerušené užívání díla objednatelem, resp. uživatelem, včetně zajištění souhlasů s autory děl v souladu s autorským zákonem.
9. Zhotovitel se zavazuje, že prováděním plnění dle této smlouvy nezasáhne neoprávněně do autorských práv třetí osoby. Odpovědnost za neoprávněný zásah do autorských i jiných práv třetích osob nese výlučně zhotovitel.

IX.
Odpovědnost za škodu

1. Zhotovitel bude povinen nahradit objednateli v plné výši škodu, která vznikla při realizaci a užívání díla z důvodů na straně zhotovitele nebo jako důsledek porušení povinností a závazků zhotovitele dle této smlouvy.
2. *Zhotovitel prohlašuje, že po celou dobu trvání této smlouvy (resp. po dobu plnění svého závazku z této* smlouvy až do doby ukončení poskytování servisní a technické podpory) bude mít sjednánu pojistnou smlouvu pro případ způsobení škody třetí osobě s limitním plněním na jednu pojistnou událost minimálně 5 mil. Kč.
3. V případě, že při činnosti prováděné zhotovitelem dojde ke způsobení škody objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu odstavce 2 tohoto článku, bude zhotovitel povinen tyto škody uhradit z vlastních prostředků.
4. Pokud v důsledku porušení povinností zhotovitele stanovených touto smlouvou nebude objednateli uhrazen finanční podíl z IROP na projektu, je zhotovitel povinen uhradit objednateli takto způsobenou škodu, a to ve výši celého podílu spolufinancování z IROP na projektu týkajícího se předmětu plnění dle této smlouvy ve výši, kterou vyčíslí odbor evropských projektů KÚ MSK a písemně sdělí zhotoviteli.
5. Zhotovitel je povinen předat objednateli na výzvu před podpisem této smlouvy a dále na vyžádání objednatelem kdykoliv v průběhu plnění závazku ve fázi I – realizační a implementační z této smlouvy ověřenou kopii pojistné smlouvy na požadované pojištění dle odst. 2 tohoto článku včetně všech dodatků a dále certifikáty příslušné pojišťovny prokazující existenci pojištění po dobu plnění závazku ve fázi I – realizační a implementační (dobu trvání pojištění, jeho rozsah, pojištěná rizika, pojistné částky, roční limity a sublimity plnění a výši spoluúčasti). Certifikát dle předchozí věty nesmí být starší jednoho měsíce.

X.
Záruka za jakost, záruční podmínky, vady díla

1. Zhotovitel odpovídá za to, že dílo má vlastnosti a funkční specifikaci stanovené touto smlouvou a že je způsobilé pro použití ke sjednanému účelu.
2. Objednatel má právo z vadného plnění z vad, které má dílo při převzetí objednatelem, byť se vada projeví až později. Objednatel má právo z vadného plnění také z vad vzniklých po převzetí díla objednatelem, pokud je zhotovitel způsobil porušením své povinnosti. Projeví-li se vada v průběhu 6 měsíců od převzetí díla objednatelem, má se zato, že dílo bylo vadné již při převzetí, neprokáže-li zhotovitel opak.
3. Zhotovitel poskytuje objednateli na provedené dílo záruku za jakost (dále jen „záruka") ve smyslu § 2619 a § 2113 a násl. občanského zákoníku, a to v délce 60 měsíců (dále též „záruční doba"). Záruční doba začíná běžet od předání a převzetí díla objednatelem. Záruční doba se staví po dobu, po kterou nemůže

objednatel dílo řádně užívat pro vady, za které nese odpovědnost zhotovitel. Pro nahlašování a odstraňování vad v rámci záruky platí podmínky uvedené v čl. XI odst. 2 a násl. této smlouvy.

4. Po dobu záruční doby ručí zhotovitel za to, že jím provedené dílo bude mít vlastnosti stanovené technickými normami platnými ke dni jeho předání a také vlastnosti pro něj obvyklé a bude plnit zvláštní požadavky dohodnuté v technické specifikaci díla, která tvoří přílohu č. 1 této smlouvy a bude způsobilé pro použití ke smluvenému či jinak obvyklému účelu.
5. Záruka se nevztahuje na vady vzniklé neodborným užíváním díla nebo případným poškozením, které vzniklo prokazatelným zaviněním objednatele, resp. uživatele.
6. Vady je zhotovitel povinen odstranit ve lhůtě stanovené v této smlouvě, nedojde-li mezi smluvními stranami k dohodě o jiném termínu, a to i v případech, kdy neuznává, že za vadu odpovídá. Pokud zhotovitel ve lhůtě sjednané touto smlouvou či ujednané mezi smluvními stranami vadu neodstraní, má objednatel právo zadat odstranění vad jiné osobě a zhotovitel je povinen tyto náklady objednateli uhradit. Pokud zhotovitel prokáže, že za vady neručí, budou mu vynaložené náklady na odstranění vady proplaceny objednatelem.
7. Uplatní-li objednatel během záruční doby vady podle čl. XI odst. 2 této smlouvy, smluvní strany berou na vědomí a souhlasí s tím, že požaduje jejich bezplatné odstranění. O odstranění vady je zhotovitel povinen vypracovat písemný zápis, který předá objednateli a ten v něm vyznačí přijetí či nepřijetí tohoto zápisu. Záruční doba se prodlužuje o dobu odstranění vady (tj. o dobu od uplatnění vady do odstranění vady). V případě, že odstranění vady proběhne dodáním věci nové, místo věci neopravitelné, začíná pro tuto novou věc běžet nová záruční doba.
8. Zhotovitel je povinen odstranit vadu na své náklady v termínech stanovených v čl. XI odst. 3 této smlouvy. Zhotovitel je povinen zahájit ihned po oznámení vad, které ohrožují bezpečnost a zdraví lidí, a které se projevily v záruční době, jejich okamžité odstraňování, a tyto vady také v nejkratším možném čase odstranit.
9. V případě, že se zjištěná vada díla či jeho části ve lhůtě dle čl. XI odst. 3 této smlouvy ukáže jako vada neodstranitelná, je zhotovitel povinen dodat do 7 kalendářních dnů od zjištění této skutečnosti novou část díla tak, aby došlo k plné funkčnosti díla podle této smlouvy, nedohodnou-li se strany jinak.

XI.
Způsob nahlašování požadavků a odstraňování vad díla (reklamace)

1. Objednatel má právo uplatnit formou reklamace svoje práva z odpovědnosti zhotovitele za vady díla.
2. Reklamace (vady) a ostatní požadavky budou hlášeny objednatelem/uživatelem díla jedním z následujících způsobů:
   a) e-mailem: *support@vitkovice.com*
   b) telefonicky: *800 331 183, 606 752 654*
3. Termíny řešení budou vycházet z přílohy č. 2 této smlouvy. Ostatní nespecifikované případy bude zhotovitel řešit takto:
   - Odstraněním vady nejpozději do 5 dnů od doručení oznámení o vadě, pokud se smluvní strany nedohodnou písemně jinak.
   - V případě havárie započne s odstraněním vady neodkladně, nejpozději do 24hodin od doručení oznámení o vadě.
   - Nezapočne-li zhotovitel s odstraněním vady ve stanovené lhůtě, je objednatel oprávněn zajistit odstranění vady na náklady zhotovitele u jiné odborné osoby.
4. K uplatňování vad dle tohoto článku smlouvy je oprávněn kromě objednatele také uživatel, který bude mít předmět díla předán k hospodaření. Každé takovéto nahlášení vady se považuje za řádné uplatnění vady objednatelem ve smyslu této smlouvy.

5. Objednatel má právo na odstranění vady dodáním nové věci nebo opravou; je-li vadné plnění podstatným porušením smlouvy, má také právo od smlouvy odstoupit. Právo volby plnění má objednatel.
6. Provedenou opravu vady díla zhotovitel objednateli předá písemným protokolem.
7. Na provedenou opravu poskytne zhotovitel záruku v délce 60 měsíců. Po uplynutí každého celého kalendářního roku od předání a převzetí díla se záruka na provedenou opravu zkracuje vždy o 12 měsíců, až na konečných 24 měsíců.
8. Zhotovitel je povinen uhradit objednateli škodu, která mu vznikla vadným plněním, a to v plné výši. Zhotovitel rovněž objednateli uhradí náklady vzniklé při uplatňování práv z vadného plnění.

XII.
Ochrana osobních údajů a důvěrných informací

1. V případě, že bude při plnění předmětu této smlouvy docházet ke zpracování osobních údajů, je tato smlouva zároveň „Smlouvou o zpracování osobních údajů" ve smyslu § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „ZOOÚ"). Zhotovitel má pro účely ochrany osobních údajů postavení zpracovatele ve smyslu ZOOÚ.
2. Zhotovitel je oprávněn zpracovávat osobní údaje pouze za účelem plnění předmětu a účelu této smlouvy.
3. Zhotovitel je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění této smlouvy, za tímto účelem je oprávněn osobní údaje zejména ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv zhotovitele vyplývajících z této smlouvy, po uplynutí této doby je povinen osobní údaje zlikvidovat. Zhotovitel je povinen na vyžádání předávat zpracované osobních údaje objednateli. Zhotovitel je počínaje dnem 25. 5. 2018 povinen poskytovat objednateli nezbytnou součinnost k plnění povinností stanovených objednateli jako správci osobních údajů Nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, současně je povinen plnit veškeré povinnosti vyplývající pro něho jako zpracovatele osobních údajů z výše uvedeného nařízení.
4. Zhotovitel učiní v souladu s platnými právními předpisy dostatečná organizační a technická opatření zabraňující přístupu neoprávněných osob k osobním údajům o ochraně osobních údajů, zejména se zavazuje zabezpečit veškerá uložená osobní a citlivá data uchovávaná v dodaném systému minimálně šifrováním a auditem přístupu.
5. Zhotovitel zajistí, aby jeho zaměstnanci byli v souladu s platnými a účinnými právními předpisy poučeni o povinnosti mlčenlivosti a o možných následcích pro případ porušení této povinnosti.
6. Zhotovitel zajistí, aby písemnosti a jiné hmotné nosiče informací, které obsahují citlivé údaje, byly uchovávány v uzamykatelných skříních umístěných v uzamykatelných místnostech.
7. Zhotovitel zajistí, aby elektronické datové soubory obsahující osobní údaje byly uchovávány v paměti počítače či jiného zařízení pouze:
   - je-li přístup k takovýmto souborům chráněn heslem,
   - je-li přístup k užívání počítače či jiného zařízení, v jehož paměti jsou tyto soubory umístěny, chráněn heslem.
8. Je-li pro účel kontroly správného fungování díla, odstranění vady nebo další vývoj díla nezbytné poskytnout zhotoviteli kopii databází, souborů nebo nosičů údajů obsahujících jakékoliv údaje o činnosti objednatele a jím určených organizací, je zhotovitel povinen s takovými údaji nakládat tak, aby nedošlo k jejich úniku či zneužití.
9. Veškeré skutečnosti obchodní, ekonomické a technické povahy související se smluvními stranami, které nejsou běžně dostupné v obchodních kruzích, a se kterými se smluvní strany seznámí při realizaci předmětu smlouvy nebo v souvislosti s touto smlouvou, se považují za důvěrné informace.
10. Zhotovitel se zavazuje, že důvěrné informace jiným subjektům nesdělí, nezpřístupní, ani nevyužije pro sebe nebo pro jinou osobu. Zavazuje se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním smlouvy a za tímto účelem jsou

oprávnění se s těmito informacemi v nezbytném rozsahu seznámit. Zhotovitel se zavazuje zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost.

11. Povinnost plnit ustanovení tohoto článku smlouvy ohledně důvěrných informací se nevztahuje na informace, které:
    a) mohou být zveřejněny bez porušení této smlouvy,
    b) byly písemným souhlasem obou smluvních stran zproštěny těchto omezení,
    c) jsou známé nebo byly zveřejněny jinak, než následkem porušení povinnosti jedné ze smluvních stran,
    d) příjemce je zná dříve, než je sdělí smluvní strana,
    e) jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem na základě zákona, popřípadě, jejichž uveřejnění je stanoveno zákonem,
    f) smluvní strana sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv.
12. Povinnost ochrany důvěrných informací trvá bez ohledu na ukončení účinnosti této smlouvy.
13. Vzhledem k veřejnoprávnímu charakteru objednatele, zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

XIII.
Sankce

1. Smluvní strany se dohodly na následujících smluvních pokutách pro případ porušení jejich povinností vyplývajících z této smlouvy:
    a) V případě prodlení zhotovitele s předáním díla dle čl. V odst. 1 této smlouvy je zhotovitel povinen objednateli uhradit smluvní pokutu ve výši 0,25 % z ceny za I. fázi díla bez DPH uvedené v čl. IV odst. 1 této smlouvy, a to za každý započatý den prodlení.
    b) V případě prodlení zhotovitele s odstraněním vady díla ve lhůtách stanovených touto smlouvou je zhotovitel povinen objednateli uhradit smluvní pokutu ve výši 5.000 Kč za každý započatý den prodlení.
    c) V případě nedodržení lhůty splatnosti faktury, kterou od zhotovitele převzal objednatel k úhradě, je objednatel povinen zhotoviteli uhradit úrok z prodlení v zákonné výši.
    d) V případě porušení povinností zhotovitele dle čl. XII odst. 2 až 7 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 100.000 Kč za každý jednotlivý případ.
    e) V případě porušení povinnosti k ochraně důvěrných informací dle čl. XII odst. 9 až 12 této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ.
    f) V případě, že se zhotovitel nezúčastní pravidelných kontrolních dní dle čl. VI odst. 7 této smlouvy bez dřívějšího souhlasu objednatele, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 3.000 Kč za každý jednotlivý takto zmařený průběh kontrolního dne či jednoho každého jednání týkajícího se předmětu smlouvy.
    g) V případě, že zhotovitel nepředá či nedoručí zápis o průběhu a závěrech jednání či kontrolního dne dle čl. VI odst. 8 této smlouvy objednateli ani do pěti pracovních dní ode dne konání jednání či kontrolního dne, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč, a to za každý i započatý den prodlení s předáním či doručením tohoto zápisu.

h) Nebude-li zhotovitel dodržovat povinnosti stanovené v čl. VI odst. 9 – 12 této smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši 3.000 Kč za každý jeden zjištěný případ.

i) V případě porušení povinnosti zhotovitele dle článku IX odst. 2 této smlouvy, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 20.000 Kč za každý i započatý měsíc, v němž nebude mít uzavřenou pojistnou smlouvu se stanovenými parametry.

2. Zaplacením smluvní pokuty není dotčen nárok oprávněné strany na náhradu škody, oprávněná strana má nárok na náhradu škody vedle smluvní pokuty v plné výši.

3. Zaplacením smluvní pokuty není dotčena povinnost splnění povinnosti, která je prostřednictvím smluvní pokuty zajištěna.

XIV.
Zánik smlouvy

1. Smluvní strany se dohodly, že smlouva zaniká:

   a) dohodou smluvních stran

   b) jednostranným odstoupením od smlouvy pro její podstatné porušení druhou smluvní stranou, přičemž podstatným porušením smlouvy se rozumí zejména:

   - neprovedení díla v době plnění dle čl. V odst. 1 této smlouvy,
   - neodstranění vad díla dle čl. XI odst. 7 smlouvy do 3 měsíců po uplynutí doby plnění dle čl. V odst. 1 smlouvy,
   - nedodržení pokynů objednatele, právních předpisů nebo technických norem, které se týkají provádění díla,
   - nedodržení smluvních ujednání o záruce za jakost nebo o právech z vadného plnění,
   - neuhrazení ceny za dílo objednatelem po druhé výzvě zhotovitele k uhrazení dlužné částky, přičemž druhá výzva nesmí následovat dříve než 30 dnů po doručení první výzvy.

2. Objednatel je oprávněn od této smlouvy odstoupit v těchto případech:

   a) bylo-li příslušným soudem rozhodnuto o tom, že zhotovitel je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);

   b) podá-li zhotovitel sám na sebe insolvenční návrh.

3. Pro účely této smlouvy se pod pojmem „bez zbytečného odkladu" dle § 2002 občanského zákoníku rozumí „nejpozději do 3 týdnů".

XV.
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem, kdy vyjádření souhlasu s obsahem návrhu smlouvy dojde druhé smluvní straně, pokud nestanoví zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), jinak. V takovém případě smlouva nabývá platnosti dnem jejího podpisu smluvními stranami a účinnosti uveřejněním v registru smluv.

2. Doplňování nebo změnu této smlouvy lze provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, vzestupně číslovaných a takto označených dodatků.

3. Zhotovitel nemůže bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí z této smlouvy třetí osobě.

4. Tato smlouva je vyhotovena ve čtyřech stejnopisech s platností originálu, z toho jeden stejnopis obdrží zhotovitel a tři objednatel.

5. Smluvní strany se dohodly, že pokud se na tuto smlouvu vztahuje povinnost uveřejnění v registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), provede uveřejnění v souladu se zákonem Moravskoslezský kraj.
6. V případě, že tato smlouva nebude uveřejněna dle předchozího odstavce, bere zhotovitel na vědomí a výslovně souhlasí s tím, že smlouva včetně příloh a případných dodatků bude zveřejněna na oficiálních webových stránkách Moravskoslezského kraje. Je-li zhotovitel fyzickou osobou, bude smlouva zveřejněna po anonymizaci provedené v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
7. Nedílnou součástí této smlouvy jsou následující přílohy:

   Příloha č. 1 – Technická specifikace realizace

   Příloha č. 2 – Specifikace provozních požadavků (požadavků na technickou podporu)

   Příloha č. 3 – Minimální technické požadavky

   Příloha č. 4 – Položkový rozpočet
8. Doložka platnosti právního jednání dle § 23 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů:

   K uzavření této smlouvy má objednatel souhlas rady kraje udělený usnesením č. 40/3553 ze dne 12. 6. 2018.

V Ostravě dne: 02. 08. 2018

[redacted]

za objednatele
prof. Ing. Ivo Vondrák, CSc.
hejtman kraje

Po dobu nepřítomnosti zastoupen
Mgr. et Mgr. Lukášem Curylem
1. náměstkem hejtmana kraje

MORAVSKOSLEZSKÝ KRAJ -S- se sídlem v Ostravě

V Ostra[redacted] 14. 7. 2018

[redacted]

za zhotovitele
Ing. Vladimír Měkota
místopředseda představenstva

Ing. Milan Juřík
člen představenstva

VÍTKOVICE
VÍTKOVICE IT SOLUTIONS a.s.
Cihelní 1575/14
Moravská Ostrava
702 00 Ostrava
IČ: 29600582
DIČ: CZ29600582

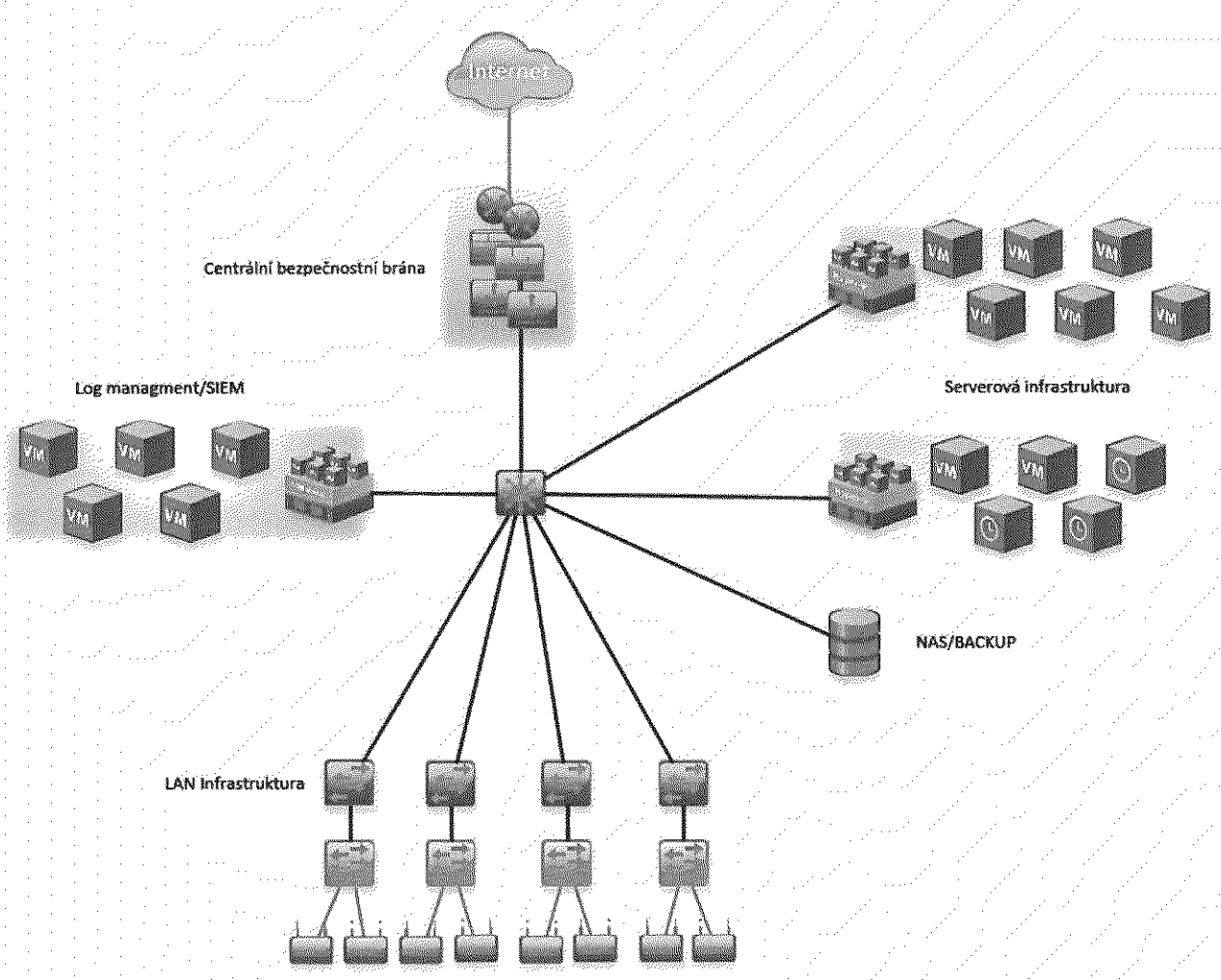
-28-

[redacted]

[redacted]

Příloha č. 1 – Technická specifikace realizace

1 TECHNICKÝ NÁVRH



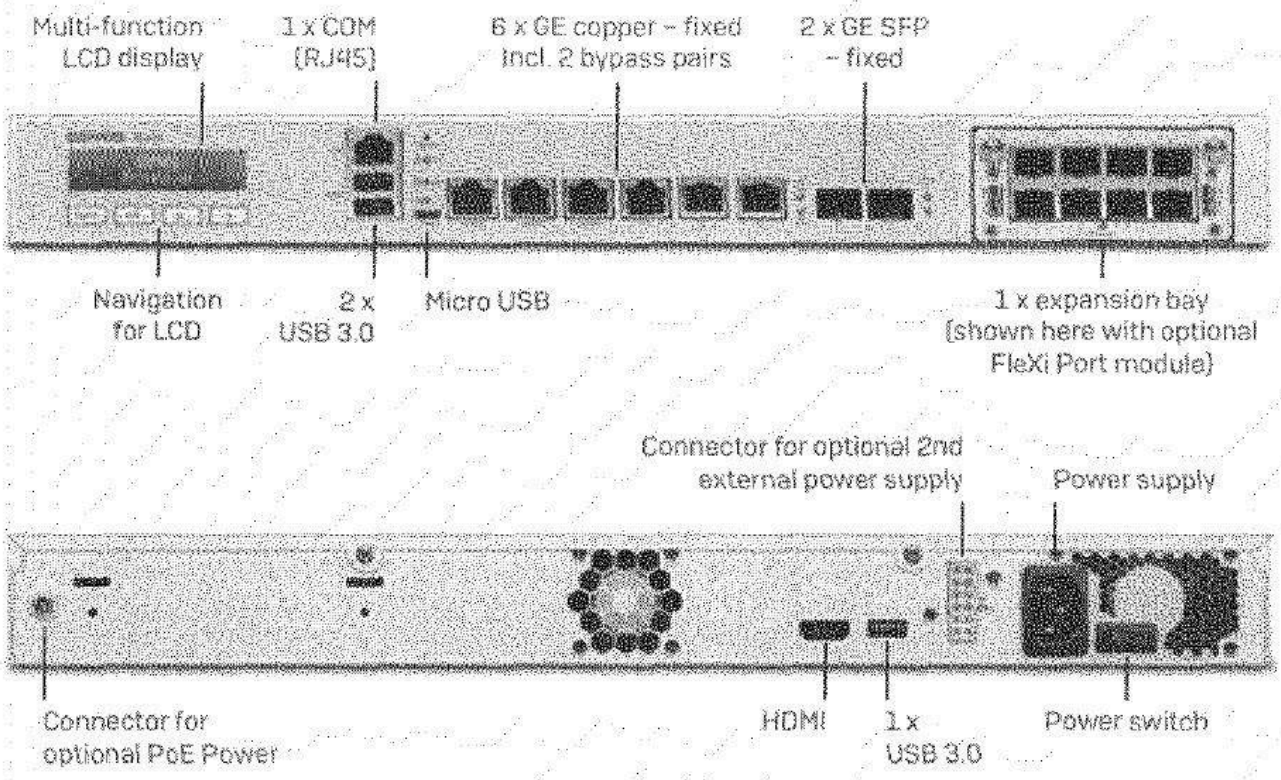
1.1 Centrální bezpečnostní brána

Perimetr infrastruktury bude tvořit **dvojice** next-generation firewall zařízení Sophos XG210, toto zařízení v sobě kombinuje funkcionality routeru, firewallu, IPS, mailové brány, webové brány a wirelless konroléru. Z důvodů vysoké dostupnosti je zvolena **dvojice** těchto zařízení pracující v režimu „failover". V případě výpadku primárního zařízení přebírá automaticky a bez-výpadkově všechny funkcionality sekundární box.

1.2 Technické parametry

Parametr	Hodnota
Propustnost firewallu	16 Gbp
VPN propustnost	1.45 Gbps
IPS propustnost	2.27Gbps

NGFW propustnost (IPS + App Ctrl)	2.2 Gbps
Antivirov propustnost (proxy)	2.3 Gbps
Počet současných spojení	8.2 mil.
Maximální počet uživatelů	neomezeně



Plná technické specifikace https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-xg-series-appliances-brna.aspx

1.3 Funkcionality

- Vytváření zón a podpora politik dle zón
- Přednastavené zóny pro LAN, WAN, DMZ,LOCAL, VPN a WiFi
- Nastavitelné zóny LAN nebo DMZ
- Routing: statický, multicast (PIM-SM) a dynamický (BGP, OSPF)
- Bridging s podporou STP a ARP broadcast forwarding
- WAN link balancing: více internetových připojení, automatická kontrola funkčnosti linky, automatické překlopení (failover), automatický a vážený balancing a podrobná vícecestná pravidla

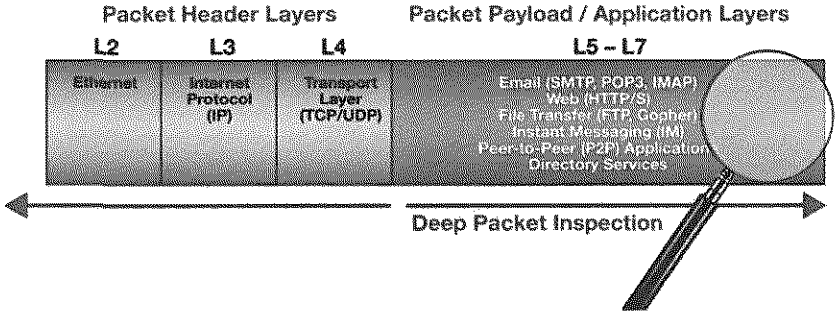
- Plná konfigurace DNS, DHCP a NTP
- Podpora a tagování VLAN DHCP
- Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- Podpora monitoringu a logování NAT (RFC 2663)
- Zařízení podporující rate limiting, antispoofing, ACL/xACL včetně všech licencí
- Možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků

- Podpora DNSSEC a IPv6 protokolů pro služby školy
- Neblokující architektura přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...
- Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let
- Podpora vzdáleného přístupu (VPN)

1.4 Bezpečnostní funkcionality

1.4.1 Hloubková analýza paketů - DPI (Deep Packet Inspection)

tato funkcionalita podrobně „nahlíží" do paketů procházejících firewallem



Díky podrobné znalosti obsahu paketu a jednoznačnému určení typu provozu a aplikace může následovat pravidlo na povolení/zakázání daného provozu na úrovni aplikace. Navíc je tato funkcionalita rozšířena o porovnávání provozu s tzv. signaturami obdobně jako u antivirových programů. Signatury jsou neustále aktualizovány a mohou odhalit probíhající útok či infiltraci sítě.

1.4.2 IPS (Intrusion Prevention System)

IPS systémy jsou považovány za rozšíření IDS systémů, protože monitorují jak provoz na síti, tak i aktivity operačního systému, které by mohly vést k narušení bezpečnosti. Hlavní rozdíl oproti IDS systémům je, že systém IPS je zařazen přímo do síťové cesty (in-line), a tak může aktivně předcházet, přípAdně blokovat detekovaný nežádoucí a nebezpečný provoz na síti. Konkrétněji, IPS může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení anebo blokování podezřelého provozu.

IPS je integrovaná součást NGFW. NGFW posílá přijaté pakety k vyhodnocení IPS, ta je vyhodnotí a v případě nezávadnosti zašle zpět. V případě závadného provozu je komunikace přerušena a incident zalogován, či odeslán administrátorům prostřednictvím mailu, nebo SNMP trapu.

Nasazení tohoto zařízení do sítě bývá problematické s ohledem na možné false-positive incidenty. Z tohoto důvodu je před samotným nasazením do sítě vhodné aplikovat tzv. transparentní mód. Pakety v transparentním módu procházejí IPS bez jejich ovlivnění, IPS je pouze vyhodnocuje a vytváří statistiky, díky kterým je nasazení do ostrého provozu jednodušší.

Pokročilá ochrana před hrozbami a synchronizovaná bezpečnost

- Detekuje a blokuje síťový provoz snažící se kontaktovat Command and Control servery využitím vícevrstvé DNS, AFC, HTTP proxy a firewallu
- Sophos Security Heartbeat okamžitě identifikuje kompromitované koncové body a zaznamenává hosty, uživatele, procesy, počty a časy incidentů
- Politiky Sophos Security Heartbeat můžou omezovat přístup k síťovým zdrojům nebo kompletně izolovat kompromitované systému do doby jejich nápravy

1.4.3 Identity firewall

V sítích uživatelé často potřebují přístup k jednomu nebo více serverovým zdrojům. Brána firewall obvykle neví o totožnosti uživatelů, a proto nemůže používat zásady zabezpečení založené na totožnosti.

Identitní brána firewall poskytuje širší řízení přístupu založené na totožnosti uživatelů. Můžeme si nakonfigurovat pravidla přístupu a pravidla zabezpečení založené na jménech uživatelů a názvech skupin uživatelů, nikoli jen prostřednictvím zdrojových Adres IP. NGFW aplikuje pravidla zabezpečení založené na přidružení Adres IP k přihlašovacím informacím služby Windows Active Directory a hlásí události založené na namapovaných uživatelských jménech namísto síťových IP Adres.

Služby firewallu založené na identitě zvyšují stávající mechanismy řízení přístupu a bezpečnostních zásad tím, že uživatelům nebo skupinám lze nastavovat firewall pravidla místo pracného zadávání zdrojových Adres IP. Politiky zabezpečení založené na identitě mohou být prokládány bez omezení mezi tradičními pravidly založenými na IP Adresách. Zakázáním uživatele v AD jsou pak i zrušena na firewallu i všechna oprávnění v síti.

- Transparentní, proxy autentizace(NTLM/Kerberos) nebo klientská autentizace
- Autentizace s podporou: Active Directory, eDirectory, RADIUS, LDAP a TACACS+
- Transparentní autentizace formou serverového agenta (STAS, SATC) s podporou Active Directory
- Transparentní autentizace formou klientského agenta s podporou pro Windows, Mac OS X, Linux
- Autentizační certifikáty pro iOS a Android
- Single sign-on: Active directory, eDirectory
- Autentizační služby pro IPSec, L2TP, PPTP, SSL

1.4.4 VPN

Na identitní firewall navazuje i funkcionalita VPN. Díky znalosti identity uživatele je možno nastavovat VPN připojení pro jednotlivé uživatele. NGFW sloužící jako VPN koncentrátor zjednodušuje správu VPN připojení do firmy. Zařazením uživatele v AD do skupiny „VPNusers", je umožněno automatické SSL VPN připojení. Následným zařazením uživatele do příslušných OU v AD jsou na něj aplikovány příslušné politiky a dle členství v konkrétních skupinách jsou uživateli umožněny přístupy k vyhrazeným zdrojům.

- IPSec, SSL, PPTP, L2TP, Cisco VPN (iOS), OpenVPN (iOS a Android)
- Bezklientský portál využívající unikátní Sophos šifrovaný HTML5 samoobslužný portál s podporou pro RDP, HTTP, HTTPS, SSH, Telnet a VNC
- VPN IPsec klient
- Autentizace: „Pre-Shared Key" (PSK), PKI (X.509), smartkarty, tokeny a XAUTH Šifrování: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (až do 2048 Bit), DH skupiny 1/2/5/14, MD5 a SHA256/384/512
- Inteligentní „split-tunneling" pro optimální směrování provozu
- Podpora NAT-traversal
- VPN SSL klient
- Osvědčené zabezpečení založené na SSL (TLS)

1.4.5 Bezpečnost webových aplikací - Web Application Firewall (WAF)

- Reverzní proxy
- Systém zabezpečení URL proti útokům typu „deep-linking" a „directory traversal"
- Systém zabezpečení formulářů

- Ochrana proti „SQL injection" útokům
- Ochrana proti „Cross-site scripting" útokům
- 2 nezávislé antivirové syst0my (Sophos & Avira)
- Převzetí šifrování HTTPS (SSL) - offloading
- Podepisování Cookie souborů digitálními podpisy
- Směrování dle obsahu (Path-based routing)
- Reverzní autentizace (offloading) pro basic autentizaci i založenou na formuláři u serverových přístupů
- Integrovaný systém rozkladu zátěže rozděluje návštěvníky na jednotlivé servery

1.4.6 Filtrování webových stránek (URL Filtering)

Tato funkcionalita umožňuje filtrovat http/https provoz dle definovaných kategorií. Firewall si z cloudu výrobce aktualizuje nevhodné stránky a zařazuje je do kategorií (hry, erotika, hazard ...)

Povolením či zakázáním jednotlivých kategorií webových stránek pro uživatele se tato pravidla aplikují na veškerý obsah v internetu.

NGFW si také pravidelně aktualizuje i seznam webů sloužících k řízení boot-netu, nebezpečné servery šířící malware atd. Při pokusu o komunikaci počítače z vnitřní sítě s takovýmto serverem je pokus o spojení automatický zablokován. Další možností je filtrování pomocí regulárních výrazů a jejich kombinací v názvech navštívených stránek.

Webová bezpečnost

- Plně transparentní webová filtrace dle uživatelů bez potřeby nastavování proxy
- Databáze URL filtrace obsahuje miliony stránek v 92 kategoriích vyvíjených a udržovaných od SophosLabs
- Politiky dle uživatelů, skupin, času či sítě
- Skenování malwaru: blokuje veškeré formy škodlivého kódu v rámci HTTP/S, FTP a webových emailů
- Pokročilá ochrana před malwarem ve webovém provozu díky emulaci JavaScriptů
- Live Protection – dotazy přes cloud v reálném čase pro nejnovější informace o hrozbách
- Druhý nezávislý antimalwarový engin od Aviry – dvojí skenování provozu
- Ochrana proti pharmingu
- Skenování HTTP a HTTPS
- Detekce a ochrana před tunelováním provozu skrze SSL
- Ověřování certifikátů

Sophos Firewall podporuje kategorizaci webových stránek

- Milióny adres URL jsou kategorizovány mezi 70 a více předdefinovanými kategoriemi
- Vlastní kategorizace je založena na klíčových slovech, názvech domén a **země původu**
- Kategorizace klíčových slov se provádí pomocí regulárních výrazů a má vyšší prioritu než shody adres URL.
- Nekompatibilní adresy URL jsou označeny jako **Nocat**
- Není-li možné kontaktovat server pro kategorizaci (sophos cloud), jsou adresy URL označeny jako **Nekategorizované (Uncat)**
- Administrátoři mohou v **zásadách** pro přístup k webu definovat akce pro **Nocat** a **Uncat**

1.4.7 AMP (Anti malware protection)

Specialisté dodavatelů NGFW řešení denně analyzují miliony vzorků malwaru. Výsledky této analýzy jsou pravidelně zasílány AMP službě zařízení. Při stažení souboru z internetu je tento soubor podroben analýze, kdy je porovnán s antivir signaturami a pomocí strojového učení a inteligentních analýz vyhodnocen. V případě jednoznačné závadnosti souboru je stažení automaticky zablokováno.

Možností rozšíření této služby je tzv. sandbox. Soubor, který je vyhodnocen jako hrozba, je nejprve odeslán do cloudu dodavatele, tam je podroben důkladé analýze a teprve v případě, že je shledán jako nezávadný, je umožněno jeho stažení.

1.4.8 DoS protection

NGFW řešení Sophos obsahuje předefinované pravidla pro anti DoS útoky

Jedná se o tyto ochrany

- SYN Flood
- UDP Flood
- TCP Flood
- ICMP Flood
- IP Flood

Kombinací sítí, na kterých je tato ochrana a parametrů jednotlivých ochran dojde k rychlému nasazení anti DoS funkcionalit

Attack Type	Source				Destination			
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)	Apply Flag	Source Traffic Dropped	Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)	Apply Flag	Destination Traffic Dropped
SYN Flood	12000	100	☐	0	12000	100	☐	0
UDP Flood	12000	100	☐	0	18000	100	☐	0
TCP Flood	12000	100	☐	0	12000	100	☐	0
ICMP/ICMPV6 Flood	120	100	☐	0	300	100	☐	0

1.4.9 Správa kvality služeb QoS a šířky pásma

QoS je síťová funkce, která umožňuje upřednostnit určité typy internetového provozu. Tato funkcionalita zabraňuje tomu, aby jeden uživatel nebyl schopen absorbovat celou šířku pásma, čímž zpomalí ostatní uživatele. QoS poskytuje funkci kontroly, která reguluje maximální šířku pásma, kterou může uživatel využívat. QoS má také možnost poskytovat lepší služby vybranému síťovému provozu. Primárním cílem QoS v je poskytnout omezení rychlosti na vybrané síťové komunikaci, aby se zajistilo, že veškerý provoz dostane svůj spravedlivý podíl omezené šířky pásma. Tok může být definován mnoha způsoby. V NGWF zařízení se QoS může vztahovat na kombinaci zdrojové a cílové IP, čísla zdrojového a cílového portu a bajtu typu služby (ToS) záhlaví IP.

Traffic Shaping je metoda, která zaručuje vztah šířky pásma mezi jednotlivými aplikacemi nebo protokoly. Jedná se o metodu řízení provozu, která vám umožňuje přidělit síťové zdroje kritickým a normálním datům na základě typu přenosu v síti a priority, kterou přidělíte tomuto provozu.
Primárním cílem zásad Traffic Shaping je spravovat a šířit celkovou šířku pásma podle parametrů, jako je uživatel, firewall, webová kategorie nebo aplikace. Politika Traffic Shaping přiděluje a omezuje maximální využití šířky pásma uživatele a ovládá webový a síťový provoz.

Šířka pásma je množství dat procházejících médiem po určitou dobu a je měřeno v kilobajtech za sekundu (KBps) nebo kilobitů za sekundu (kbitů) (1 Byte = 8 bitů).

Můžete definovat zásady Traffic Shaping pro:

Uživatel - omezuje šířku pásma konkrétního uživatele
Pravidla - omezuje šířku pásma pro entitu, na kterou se použije pravidlo brány firewall
Kategorie webu - omezuje šířku pásma pro kategorii URL kategorizovanou v kategorii webu

Nastavení jednotlivých pravidel je přehledně popsáno na webu výrobce

- Sophos Firewall: Jak omezit šířku pásma pro službu
- Sophos Firewall: Jak omezit šířku pásma na webových stránkách
- Sophos Firewall: Jak aplikovat politiku tvarování provozu pro uživatele VPN
- Sophos Firewall: Jak aplikovat omezení aplikace na šířku pásma

1.4.10 Bezpečnost Wi-Fi sítě

- Jednoduché „plug-and-play" nasazení bezdrátových přístupových bodů Sopohos
- automatické přidání do control centra firewallu
- Centrální monitoring a správa všech přístupových bodů (AP) a bezdrátových klientů přes bezdrátový kontrolér
- Integrovaná bezpečnosti: Veškerý Wi-Fi provoz je automaticky směrován přes firewall
- Silné šifrování podporuje nejvyspělejší autentizační metody vč. WPA2-Enterprise a IEEE 802.1X (RADIUS)
- Bezdrátový přístup do internetu pro hosty s funkcí „walled garden"
- Časově definovaný přístup do sítě přes Wi-Fi
- Podpora přihlášení přes HTTPS
- Vynutitelné kešování pro updaty Sophos Endpoint
- Filtrování typů souborů dle mime-type, přípony a aktivního obsahu (např. ActiveX, applety, cookies, atd.)
- Možnost vynucení YouTube pro školy
- Možnost vynucení „SafeSearch"

1.4.11 Aplikační bezpečnost

- Vylepšené řízení aplikací dle signatur a vzorů na 7. vrstvě pro tisíce aplikací. Řízení aplikací dle kategorií, charakteristik (např. šířka pásma, ztráta produktivity), technologií (např. P2P) a úrovně rizika
- Vynucení pravidel aplikační kontroly dle uživatele nebo sítě
- Možnost řízení šířky pásma pro aplikaci za účelem omezit nebo garantovat priority pro upload/download

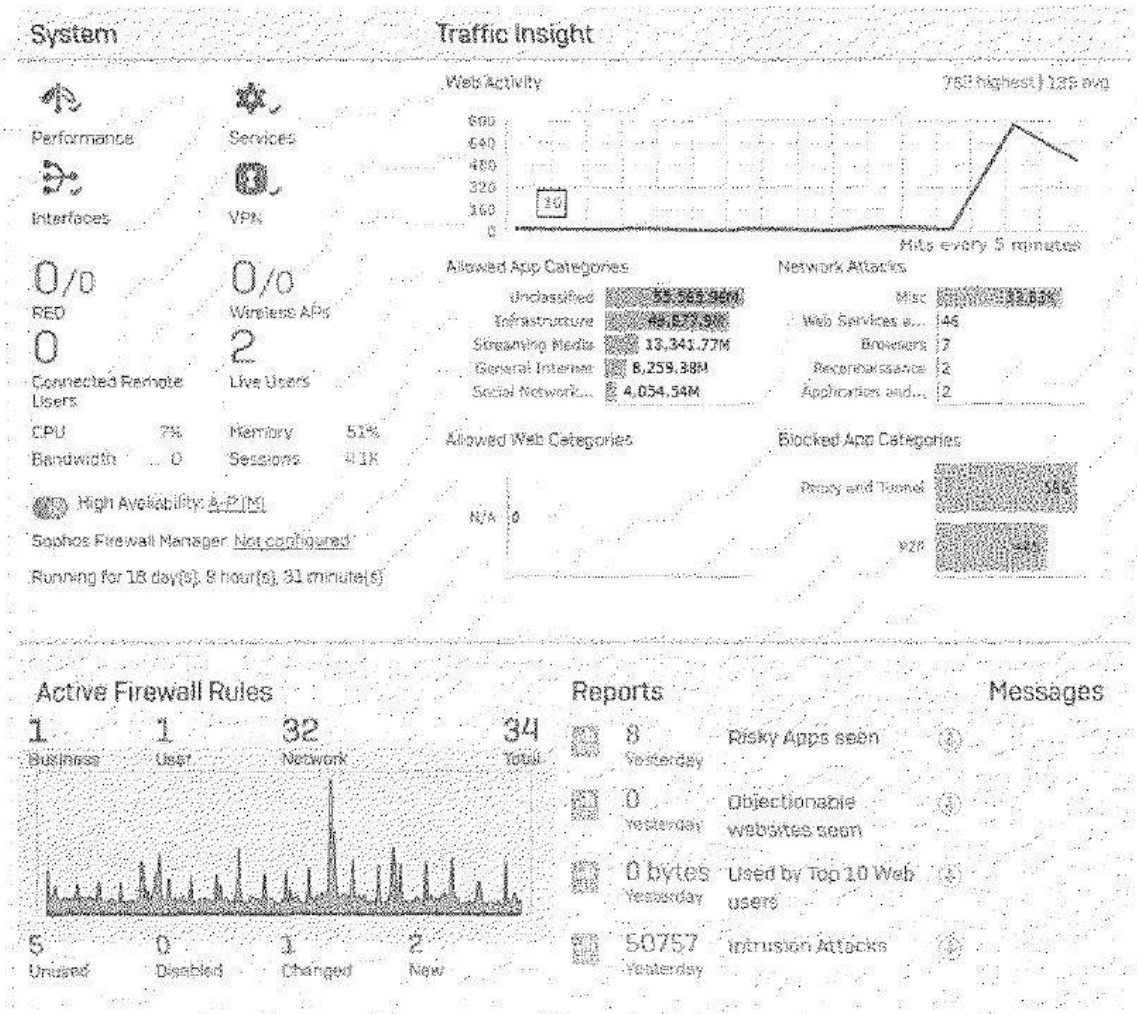
1.4.12 Emailová bezpečnost

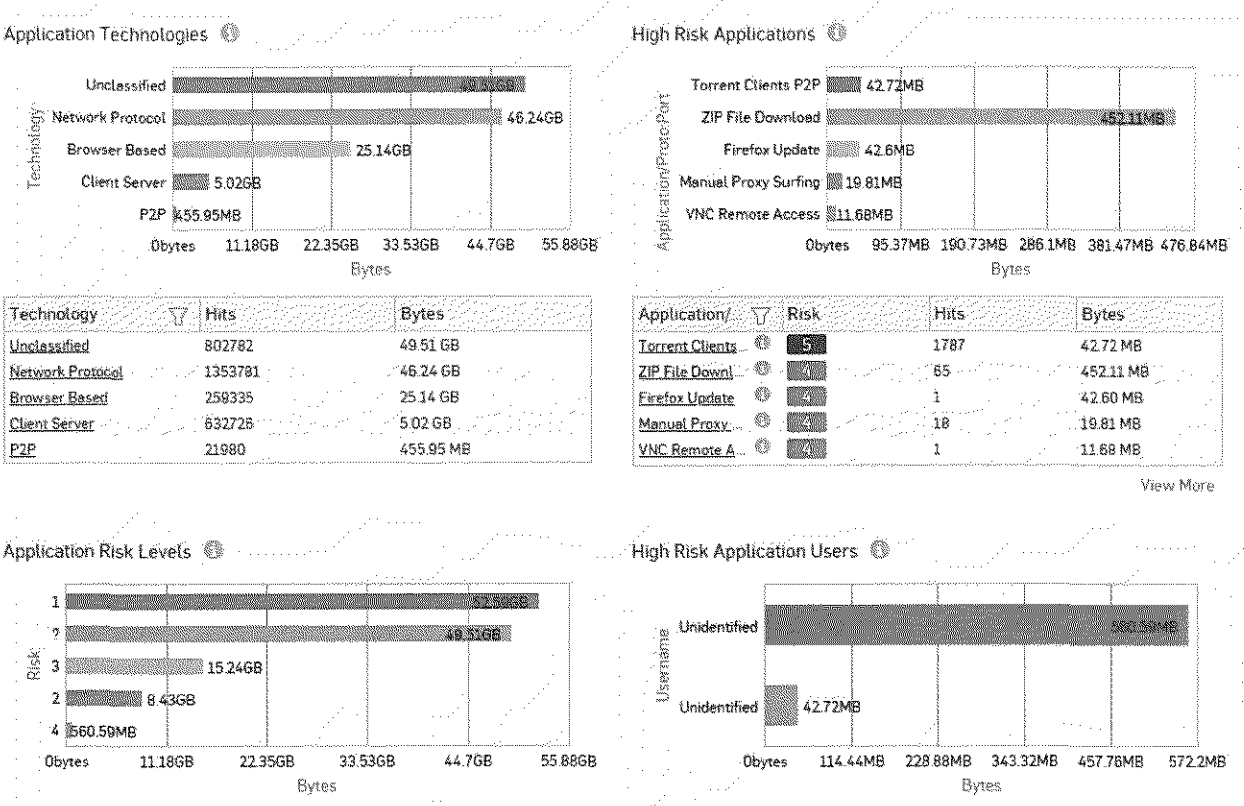
- Reputační služba s monitoringem spamových kampaní založená na patentované technologii RecurrentPattern-Detection
- Blokuje spam a malware v SMTP provozu
- Detekuje phishingové URL uvnitř emailů Black/white listy adres a domén dle uživatelů/globálně
- Skenování emailů pro SMTP, POP3 a IMAP 2 nezávislé antivirové enginy (Sophos & Avira)
- Skenuje vložená data: blokuje nebezpečné a nechtěné soubory s kontrolou typu souborů (MIME type) Karanténa pro neskenovatelné či nadměrně objemné zprávy Filtrace pošty pro neomezený počet domén a poštovních schránek
- Automatické aktualizace signatur a vzorů
- Propojení s cloudovou službou Sophos Live
- Anti-Virus pro dotazy na aktuální hrozby v reálném čase.
- Šifrování emailů a prevence úniku citlivých dat (DLP)
- Patentovaná technologie SPX (Secure PDF Exchange) pro jednosměrné šifrování zpráv
- Samoobslužná registrace SPX hesel příjemců

- Transparentní de/šifrování a podepisování SMTP emailů
- Kompletně transparentní, není třeba další software či klient
- Umožňuje skenovat obsah/viry i u šifrovaných emailů
- DLP engine s automatickým vyhledáváním citlivých dat v emailech a přílohách
- Předpřipravený kontrolní list citlivých dat (CCLs) pro PII, PCI,HIPAA a další, připravený a udržovaný od SophosLabs
- Uživatelský samoobslužný portál
- SMTP karanténa: prohlížení a uvolňování zpráv z karantény

1.4.13 Logování a reportování

Díky nasazení Next-Gen firewall řešení na místo centrální bezpečnostní brány a routeru zároveň je na NGFW zajištěno logování packetů procházejících skrze LAN/WAN/WIFI sítě. Tato trajektorie packetu skrze sítě je navíc doplněna o znalost identity uživatele, znalostí aplikací, které spolu komunikovali. Další výhodou tohoto logu je okamžitý přehled na dění v sítích, informování správců o útocích a zranitelnosti. Nad těmito informacemi je snadné vytvářet nová bezpečnostní pravidla pro bezpečnější chod sítí. Provozní logy budou z NGFW zasílány na LogServer, kde lze generovat přehledné reporty.





Technology	Hits	Bytes
Unclassified	802782	49.51 GB
Network Protocol	1353781	46.24 GB
Browser Based	259335	25.14 GB
Client Server	632726	5.02 GB
P2P	21980	455.95 MB

Application/...	Risk	Hits	Bytes
Torrent Clients ...	5	1787	42.72 MB
ZIP File Downl...	4	65	452.11 MB
Firefox Update	4	1	42.60 MB
Manual Proxy ...	4	18	19.81 MB
VNC Remote A...	4	1	11.68 MB

View More

- Stovky reportů na zařízení s možnostmi vlastního nastavení
- Anonymizuje data
- Plánování reportů pro různé příjemce dle skupin reportů s flexibilní periodou
- Nastavitelná délka uchování logů dle kategorií
- Dashboardy pro síťový provoz, bezpečnost a ukazatel rizik spojených s uživateli
- Aplikační reporty pro rizika uživatelských aplikací, blokované uživatelské aplikace, webová rizika, blokované přístupy na web, vyhledávací enginy, využití webového serveru, ochranu webového serveru, přenos uživatelských dat, FTP provoz
- Síťové reporty a reporty hrozeb pro útoky-narušení sítě, pokročilou síťovou ochranu, Wi-Fi a Security Heartbeat
- Reporty využití a ochrany emailu
- reporty shody pro HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3 a CIPA
- Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- Zabezpečení přístupových protokolů (SSL/TLS), antivirová ochrana webových systémů
- Statistiky přístupu uživatelů k internetovým serverům
- Export logů v PDF

1.4.14 Managment

- Uživatelsky komfortní rozhraní
- Navigace v GUI na 3 kliky kdekoli
- Kontextová nápověda u každé položky menu
- Pokročilé nástroje pro řešení problému v GUI (např. Packet Capture)

- Administrace dle rolí – selektivní definice oprávnění
- Automatické upozornění na aktualizace
- Objektově orientovaný systém definice pro sítě, služby, hosty, časové úseky, uživatele a skupiny, klienty a servery
- Sledování změn v konfiguraci
- Upozorňování skrze email nebo SNMP trapy

2 LAN infrastruktura

2.1.1 Managment

Managment přístup na LAN prvky (HTTPS, SSH) a autorizace uživatelů bude řešena pomocí protokolu 802.1X (Radius). V AD bude zřízena skupina specifická skupina, do které budou přiřazení oprávnění uživatelé. Těmto uživatelům bude nastaveno konfigurační oprávnění (admin/

2.1.2 Zálohování konfigurací LAN prvků

Konfigurace dodaných LAN prvků budou pravidelně zálohovány a konfigurace budou ukládány na NAS

3 Bezdrátová LAN

Funkce bezdrátového kontroléru je implementována v centrální bezpečnostní bráně (Sophos XG210) Díky této implementaci je možno aplikovat veškeré next-gen firewall funkcionality i na bezdrátovou síť což zjednodušuje správu bezdrátové sítě.

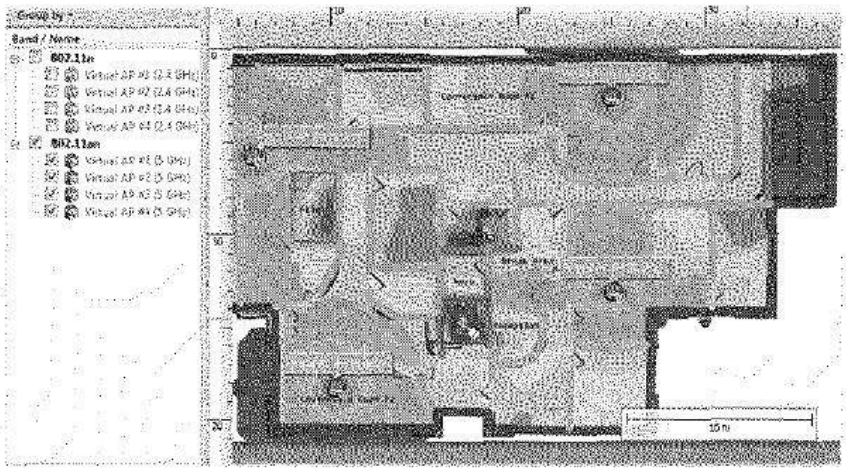
V bezdrátové LAN budou použity AP100. Nasazení AP probíhá zcela automaticky. Po připojení AP do sítě je nové AP detekováno centrální bezpečnostní bránou. Schválením nového AP v bezdrátové síti jsou automaticky aplikovány bezpečnostní nastavení bezdrátové sítě.

Specifikace AP

https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-wireless-dsna.pdf

https://www.cyberoam.com/downloads/Sophos/Specsheet/AP100Specsheet.pdf

Umístění AP v budovách školy bude předcházet prediktivní simulace šíření signálu ve specializovaném software. Tato simulace navrhne vhodné umístění instalace AP.



3.1 Guest Access

Pro funkcionality bezdrátové LAN spojené s přihlašováním „Guest" uživatelů, bude v serverové infrastruktuře instalován software ICA-BOX (Internet for Guest). Tento software zajistí

- Předdefinované přihlašovací stránky včetně textů, a překladů do 24 jazyků
- Funkce "Remember Me" pro automatickou relogin
- Dynamické řízení šířky pásma vč. garantované šířka pásma na návštěvníka

- Předdefinované podmínky použití pro všechny dostupné jazyky
- Individuální billing (čas, objem dat, šířka pásma)
- Simultánní přihlášení na více zařízeních se stejnými přihlašovacími údaji
- Scan & Surf (přihlášení pomocí QR kódu) Grafický tisk lístku vč.QR kódu s logem školy
- Walled Garden (zdarma dostupné webové stránky pro všechny)
- Skutečný Plug & Play Engine - není potřeba měnit síťová nastavení v zařízeních návštěvníků
- Protokolování všech příslušných akcí
- Velký počet PMS rozhraní (Micros Fidelio, Protel, ...)
- Online platební rozhraní (platební karty včetně PayPal)
- Externí ověřování pomocí databází, LDAP (včetně MS Active Directory), Radius a iPass
- Přihlašování prostřednictvím social media účtů (Facebooku,Google ..)
- vyžádání přihlášení pomocí SMS nebo e-mailu
- Požadavek na vstup prostřednictvím e-mailu (aktivace návštěvníka mailem)
- Uživatelský agent Autologon (volné přihlášení podle prohlížeče User-Agent)

Specifikace

https://www.iacbox.com/en/products/datasheets/?no_cache=1&tx_bh_page%5Bfile%5D=598&tx_bh_page%5Baction%5D=download&tx_bh_page%5Bcontroller%5D=File

3.2 Výkonnostní/licenční dimenzování

Bezdrátové řešení obsažené v této nabídce je licenčně a výkonnostně dimenzováno

- 75 ks AP na bezdrátovou LAN
- 8 SSID na AP
- 16 SSID na bezdrátovou LAN
- 1.3 Gbps (5GHz / 802.11ac) + 450 Mbps (2.4GHz / 802.11n) per AP
- počet uživatelů na AP není omezen

4 Logování provozu - SIEM

V moderní LAN infrastruktuře je nezbytné zaznamenávat události spojené s provozem.

Jedná se zejména o

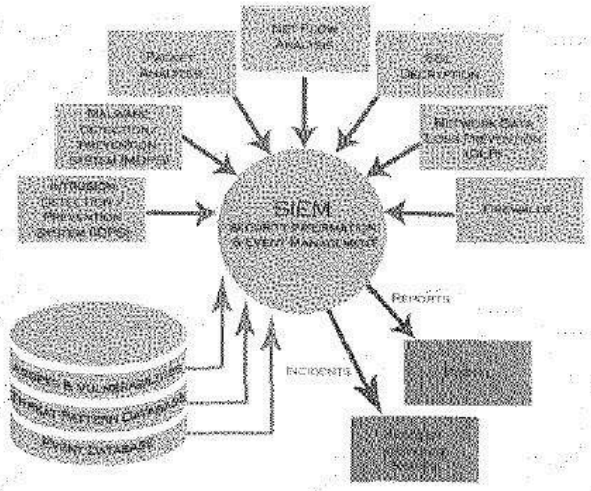
- Přístupy uživatelů k aktivním prvkům
- Konfigurační změny
- Systémové události na aktivních prvcích
- Bezpečnostní incidenty

Aktivní prvky mají tyto události zaznamenávat a automaticky odesílat nadřazenému systému. Pro komunikaci mezi aktivními prvky a centrálním logovacím systémem bývá nejčastěji používán protokol syslog.

Problémem však bývá spojit jednotlivé události z aktivních prvků do souvislostí. Díky potřebě uceleného pohledu nad událostmi v LAN byl po roce 2005 vyvinut systém SIEM (Security Information and Event Management), který poskytuje rozšířené funkcionality logování jako

- Agregace dat - seskupení vybrané části určitých entit za účelem vytvoření nové entity. Jednotlivými entitami mohou být např. data z přepínačů, firewallů, serverů, počítačových stanic, databází, IDS/IPS, aplikací atd.
- Korelace - nalézání vzájemných vztahů událostí, např. monitorování činnosti konkrétního uživatele, pohled na určité události v nějakém časovém intervalu atp.
- Varování (alerting)
- Informační panely, přehledové sestavy (dashboards)
- Reportování shod (compliance)
- Archivace, ukládání historických dat (logů)

Tento nástroj umožňuje administrátorům pružnější a rychlejší reakce na útoky, včasnou detekci útoků a zefektivnění správy infrastruktury. Na systém SIEM je navíc možno směrovat logovaní dalších systémů (firewall, Flow monitoring, Active Directory ...), a tím zajistit komplexní přehled nad infrastrukturou LAN z jednoho místa.



Obrázek – Princip SIEM integrace

4.1 SIEM – HW parametry

Siem řešení bude instalováno na vyhrazeném serveru DELL PowerEdge R440 Server
2x CPU Xeon 3104 1.7GHz
64GB RAM
2x16 GB SD RAM virualization OS
480GB SDD Virtal server OS
1TB SATA SIEM Data

Na tomto serveru bude instalována virtualizační platforma VMware ESX 6.5U1. Ve virtualizaci bude instalován Open-Source řešení SIEMonster

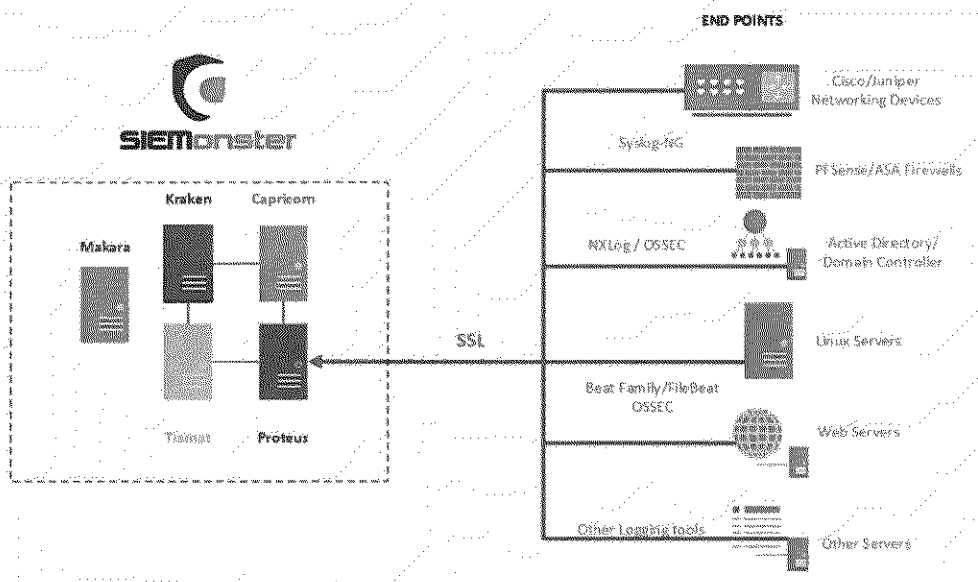
Specifikace serveru

http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/PowerEdge-R440-Spec-Sheet.pdf

4.2 SIEM - technické řešení

SIEMonster je komplexní Enterprise Security Information and Event Management (SIEM), postavený na škálovatelných, open-source součástech vyvinutých komunitou a týmem SIEMonster. SIEMonster byl vyvinut jako plná náhrada komerčních řešení SIEM. Produkt je bezplatný, plně zdokumentovaný, neexistují žádné omezení dat nebo endpoint zařízení.

Architektura SIEM bude řešena 5-ti servery v clusteru (Makara, Kraken, Tiamat, Capricorn, Proteus) pojmenovaných podle mytologických postav.



- Makara - Orchestrator
- Proteus - Log kolektor
- Capricorn - Korelace a prohlížení logů
- Kraken - Database Cluster Node 1
- Tiamat - Database Cluster Node 2

4.3 SIEM - Přehled logovacích funkcí

Multiple Domain Controllers Security Event Logs	Administrator Actions	SOC Dashboard with breakdowns of relevant DC security Events
External Websites IIS & Apache	Logon Failures	2007, 2010 Microsoft Exchange Dashboards for Tracking Logs
Exchange OWA and Message Tracking	Anomalous Activity – Spikes/Flatlines	Exchange OWA Activity
Multiple Cisco Devices	Brute force attacks	External Website Dashboards for IIS and Apache
IPS devices	Multiple Logon Source IPs	Cisco, Juniper
VPN Concentrators	Email phishing and virus attacks	Linux, Windows, Unix, Apple
Internal Asset Vulnerability Analysis Data	Denial of Service Attacks	Antivirus
Bluecoat Proxy	Web Application Hacking Attempts	OSSEC HIDS
Ironport Firewalls	Honeypot activity	Bluecoat Proxy
McAfee ePO Orchestraior	HIDS	Syslog
OSSEC HIDS Data	Virus Outbreaks	Vulnerability Data
Any device that's produce a log, syslog snmp or agent installed	Heartbeat	Anything that logs, you can visualize

4.4 SIEM – výkonnostní dimenzování

Řešení je dimenzováno

- 1000 monitorovaných endpoint zařízení
- 47 mil událostí za hodinu cca 13 tis EPS (event per second)

Systém není licenčně omezen na počet logovaných endpoint zažízení nebo EPS

4.5 SIEM – log kolektor

Aktivní prvky LAN (Router, Firewall, Switch, WIFI) podporující **syslog** zprávy budou předávat lokální logy SIEM kolektoru, portem UDP/514 ev. TCP/514
Windows server odesílají lokální logy SIEM řešení prostřednictvím instalované služby **NXlog**
Linux server odesílají logy centrálnímu SIEM řešení prostřednictvím služby **filebeat.**

NXlog a **filebeat** komunikace probíhá šifrovaně, šifrování je řešeno SSL protokolem a certifikátem na endpoint zařízení.

Nasbírané aletry jsou ukládány do centrálního SIEM logu ve standartizovaném formátu, nad nasbíranými logy probíhá agregace a korelace dle přednastavených pravidel za účelem odhalení závadného prvozu.

5 Monitoring sítě

Pro monitorování, sběr provozních veličin aktivních prvků a reporting dostupnosti jednotlivých zařízení bude použit open-source monitorovací nástroj Centreon. Tento software vychází z monitorovacího systému NAGIOS, který byl však upraven pro jednodušší správu a dopiněn automatizací procesů, škálovatelností a integrací s dalšími open-source produkty pro monitoring podnikových IT systémů

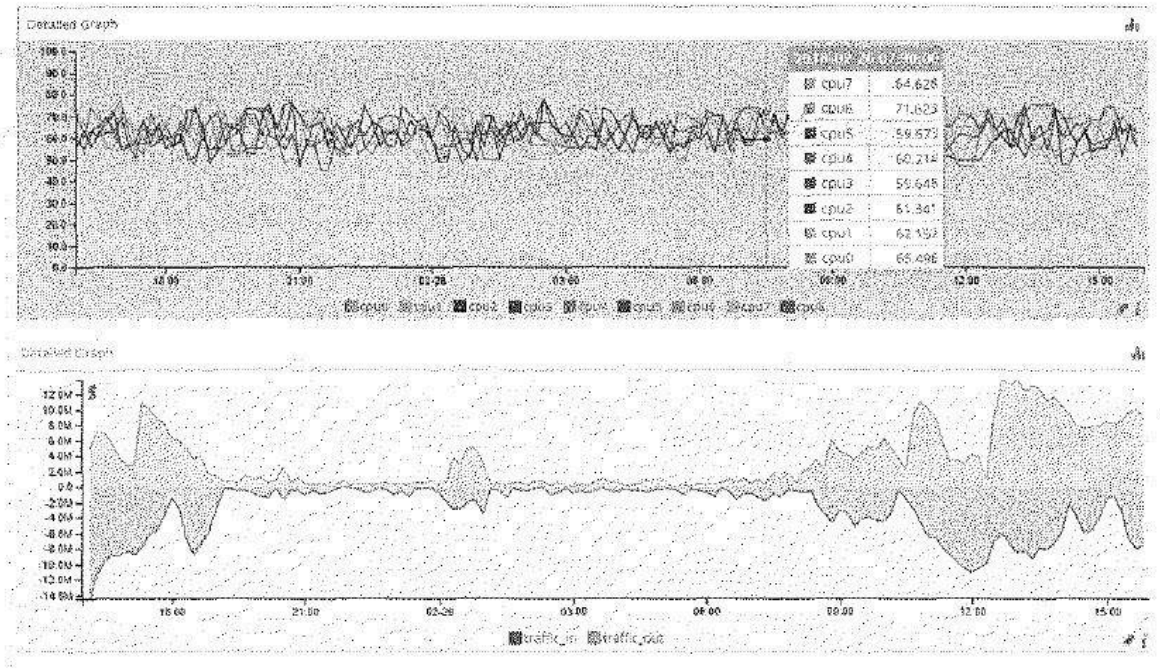
5.1 Funkcionality

- monitoring dostupnosti síťových periferií (echo request = ping)
- monitoring dostupnosti služeb (SMTP, FTP, HTTP, SSH a mnoho dalších)
- monitoring systémových údaje síťových zařízení podporující SNMP (verze 1-3) a SNMP trap
- podpora pluginů - možnost jednoduchého dopsání vlastních monitorovacích skriptů
- notifikace přes e-mail, SMS, pager
- Plánované akce nad událostí z monitoringu (spustit script, restartovat, vypnout...)
- podrobné statistiky a záznamy událostí
- grafické rozkreslení topologie sítě ve 2D, ale i 3D
- vzdálená správa pomocí webového rozhraní
- přívětivé webové prostředí
- monitorovaná data jsou uchovávána v SQL DB
- možnost přídavných modulů
- správa logů, statistik a grafů
- jednoduchá aktualizace

Monitoring aktivních prvků sítě a sběr provozních hodnot bude zajištěn následujícími komponenty

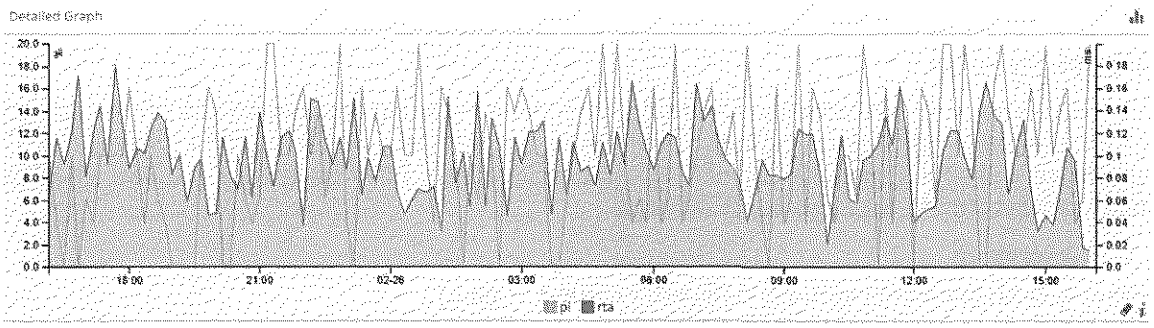
5.2 Performance monitoring

Sběr informací o provozním vytížení aktivních prvků (CPU, MEM), přenosových statistikách (LAN, WAN, WIFI). Provozní informace jsou z aktivních prvků vyčítány pomocí SNMP protokolu. Z nasbíraných údajů jsou generovány reporty a přenosové statistiky v grafické podobě



5.3 Monitoring dostupnosti

Prostřednictvím kontrol v nastavených periodách je zjišťována informace o dostupnosti aktivních prvků (ICMP, SNMP) a služeb na nich běžících (DNS, DHCP, SSH..) V případě nedostupnosti je vyhlášen poplach. O nedostupnosti jsou informování správci prostřednictvím SMS a mail notifikací. Samozřejmostí je reporting a grafické přehledy o dostupnosti



6 SW pro audit a správu ICT prostředků

Pro audit software a evidenci hardware bude použit software AW Caesar
Scanery HW a SW provádí scanování dat na počítačích uživatelů. Data se shromažďují a předávají k analýze dle vědomostní databáze. Automaticky na pozadí probíhá vyhodnocení HW a SW a pak se data ukládají do evidenční části programu. Sběr dat je možný prostřednictvím počítačové sítě, e-mailem, FTP rozhraním i USB Store. Správce IT pak provádí průběžnou kontrolu aktuálního stavu SW, licencí a HW.
V kombinaci s GPO je možné doplnit funkcionality o instalace schválených SW dle IT směrnic.

6.1 Funkcionality

6.1.1 Definice rolí

Pro uživatele lze jednoduše nastavit přístup do tabulek, datových položek, filtrů, výběrů, tisků i exportů. Toto nastavení lze přenášet jednoduše na další uživatele. Lze vytvořit více typových rolí. Úspora času na údržbu práv uživatelů.

6.1.2 Nový systém konfigurací

tzv. dědičné konfigurace. Základní typy konfigurací Správce (admin) a Uživatel, které nastavují základní prostředí programu. Filtry, pohledy, třídění. Vždy platí poslední konfigurace. Úspora času správce systému.
Definování zástupce odpovědné osoby.
Možnost přístupu jiné osoby do konkrétních dat. (zástup z dovolenou, nemocenskou, společné databáze). Tři typy úrovně rozsahu práv, případně časové omezení.

6.1.3 Zcela nový způsob pohledů na data.

- rychlejší zobrazení položek
- různé definice pohledů na data
- uživatelské uložení pohledů
- možnost přednastavení výběru pohledu při spuštění (úspora času uživatele)

6.1.4 Nové uživatelské filtry dat

- jmenné
- interaktivní
- možnost uživatelského ukládání filtrů
- nové rychlé vyhledávání v kterékoliv položce s hvězdičkovou konvencí

6.1.5 Manažerské multi-pohledy

- veškeré nastavení výběru (filtr, třídění, výběr položek, grupování) se uživatelsky uloží pod názvem

- možnost zaslání odkazu na daný výběr e-mailem konkrétní osobě. Té se data zobrazí, dle jejich oprávnění. Tedy zobrazí se mu jen ty položky, které smí vidět.
- možnost ukládání různých kombinací výběru dat (operativní, rychlé a efektivní výběry potřebných dat)
- úspora času vedoucích pracovníků

6.1.6 Logování přihlášení odpovědných osob

- jednoznačná identifikace autora změny v datech (vyšší bezpečnost dat)
- Spouštění více záložek v prohlížeči
- možnost současného zobrazování různých pohledů na data a jejich vzájemné porovnávání.

6.1.7 Zcela nový tiskový systém

- plně lokalizovaný
- výstupy tisků do PDF, html, word, excel
- ukládání tisku
- elektronické předávací protokoly

6.1.8 Uživatelské exporty dat

- zobrazení a exporty dle uživatelského oprávnění
- položky uživatelsky vybíratelné
- filtry, pohledy, výběry

6.1.9 Automatická analýza a přihrání scanovaných dat

- zcela nová optimalizovaná koncepce - víceprocesorové zpracování
- rychlejší analýza a přihrávání zpracovávaná na pozadí
- možnost automatizovaných hromadných dávek
- nastavení zpracování na čas
- zpracování průběžného zpracování dle nových dat scanů
- neustálá dostupnost systému
- snížení zatížení sítě přenosy
- zvýšení operativnosti

6.1.10 Definice obrazovek dle požadavku uživatele

uživatel si definuje vlastní nastavení prostředí, zobrazení dat, různé výběry, které je možno uložit.

6.1.11 Systém a datové prostředí

AW Caesar pracuje v prostředí Firebird verze 2.5, který využívá více procesorů a tím je propustnější pro více současně pracujících uživatelů.

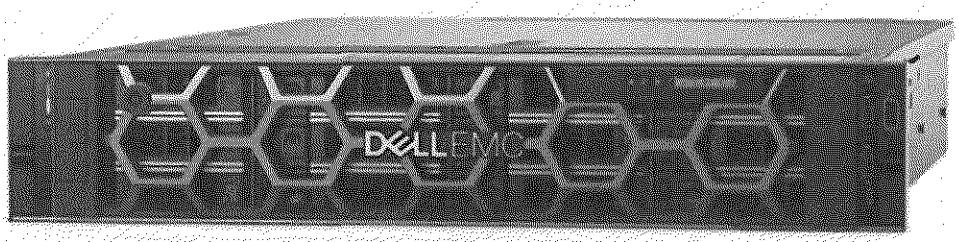
Celý systém umožňuje libovolný výběr a použití dat, což umožňuje ideální spolupráci s dalšími aplikacemi (SAP, GINIS, HP Help Desk, CA – Help Desk a jiné systémy.

- Všechny údaje jsou uloženy v jedné databázi
- Evidenční část je řešena databází FireBird 2.5
- HW Scanner získává podrobné informace o HW, není potřeba jej na stanici instalovat
- Velká databáze SW vzoru - více než (přes 1 600 000 souborů k 1.1.2018.) Aktualizace se provádí prostřednictvím internetu
- Dodané základní sestavy + Uživatelský generátor sestav
- Možnost certifikace uživatelských SW vzoru, zasílání podkladů pro SW Vzory, sledování požadavků uživatelů přes webové rozhraní
- Možnost jednoduché tvorby vlastních SW vzorů

- Analýza SW upozorňuje i na zcela neznámé SW nenacházející se v databázi SW vzorů

7 Serverová infrastruktura

7.1 HW Parametry



Dvojice serverů DELL PowerEdge R540 server

2x CPU Intel Xeon Silver 4110 2.1G, 8C/16T – 36678 bodů
64GB RDIMM, 2667MT/s
2x480GB SSD SATA, RAID 1, Virtal server OS
2x8TB 7.2K RPM SATA RAID 1, Virtual server data
Redundantní napájení - PWR SPLY,750W,RDNT,DELTA

7.2 Virtualizace

Na serverech DELL R540 bude instalována virtualizační platforma Hyper-V ve verzi 2016

7.2.1 Hyper-V

Virtualizační platforma Microsoftu pokrývá široké spektrum potřeb, od nejjednodušších scénářů konsolidace několika serverů až po vysoce výkonná, škálovatelná a samoobslužná datová centra o stovkách a tisících serverů.

7.2.2 Charakteristika Hyper-V

Základním stavebním kamenem je virtualizační vrstva neboli hypervisor Hyper-V, který ve své první verzi spatřil světlo světa v roce 2008 jako součást některých edic Windows Serveru 2008. Následovala druhá generace, dostupná jako role ve Windows Serveru 2008 R2, případně jako samostatný produkt Microsoft Hyper-V Server 2008 R2, který je k dispozici zdarma. Funkcionalitu doplnily technologie Dynamic Memory a RemoteFX, obsažené v Service Packu 1 pro Windows Server 2008 R2. Následovala třetí generace Hyper-V, jež je integrovanou součástí Windows Serveru 2012 a klientského operačního systému Windows 8 Pro. Aktuálně je k dispozici Hyper-V coby integrovaná součást Windows Serveru 2012 R2 a Windows 8.1 Pro a Enterprise. Zkušební verze serverů můžete stáhnout na této stránce v sekci "Vyzkoušejte zdarma".

V rámci Hyper-V jsou podporovány následující opračních systémy:

- Windows Server od verze 2003 výše
- Windows Client od verze XP Professional SP2 výše
- SUSE® Linux Enterprise Server verze 10 a 11
- Oracle Linux 6.4 a vyšší
- Open SUSE 12.3
- Red Hat Enterprise Linux verze 5.5 a vyšší
- CentOS Linux 5.5 a vyšší
- Ubuntu 12.04 a vyšší
- FreeBSD 8.2
- Debian 7.0 a vyšší

7.2.3 Hyper-V vlastnosti

- Microsoft Hyper-V Server k dispozici zdarma.
- Integrovaná součást Windows Serveru 2016
- Snadná konsolidace serverů.

- Bezproblémová rozšiřitelnost.
- Vysoká dostupnost součástí řešení.
- Využití od nejmenších prostředí po velká datacentra.
- Efektivní správa pomocí System Center.
- Základní stavební kámen privátního cloudu (Hyper-V cloud).

7.2.4 Windows Server 2016 Hyper-V posouvá limity využitelnosti ještě dál

- Až 1000 hostů na jednom hostiteli
- Až 8000 hostů v rámci clusteru, který může mít až 64 nodů
- Využití až 320 procesorových jader a 4 TB paměti pro Hyper-V roli na fyzickém hostiteli
- Přidělení až 64 virtuálních procesorů, 1 TB paměti a 255 disků (každý až o velikosti 64 TB) pro systém ve virtuálním prostředí

Díky pokročilým technologiím pro dynamickou správu paměti, odděleného síťového provozu, podpoře síťových úložišť a dalších technických vymožeností lze Hyper-V využít jak při základní konsolidaci serverů v malé firmě, tak pro vybudování datacentra o tisících fyzických serverech, kde se úspěšně využívají možnosti vysoké dostupnosti typu Hyper-V clusterů, Live Migration a dalších.

7.3 Virtuální servery specifikace parametrů

7.3.1 AD – Active Directory

Adresářová služba Active Directory je rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře.

7.3.1.1 Příprava implementace AD

Pro zodpovědné naplánování a vytvoření funkční holdingové infrastruktury opírající se o Active directory budeme potřebovat se zadavatelem projít organizační strukturu školy, požadavky na zabezpečení, delegaci správy AD. Tato fáze je důležitá pro dobře a logicky navrženou infrastrukturu AD. Součástí této přípravné fáze musí být ověření kompatibility stávajícího aplikačního softwarového vybavení s novou AD strukturou.

7.3.1.2 Implementace AD

Vlastní implementace AD doporučujeme realizovat na Microsoft Windows serveru 2016 a sice kombinací doménových řadičů, které budou nasazeny ve virtuálním prostředí a minimálně jednoho řadiče, který bude ve virtuálním prostředí a bude tedy virtualizován. Jako optimální se jeví varianta s dalším doménovým řadičem, který bude nainstalován v režimu RODC tzn. Read-Only. RODC řadič poskytuje klientům standardní služby jako klasický doménový řadič, ale jeho nasazení se doporučuje do prostředí s nižším stupněm fyzické bezpečnosti.

Vlastní adresářová struktura a jednotlivé OU budou korespondovat se stávající organizační strukturou školy. Doporučujeme vždy zřízení samostatných containers jak pro uživatelské účty, tak pro účty pracovních stanic a sice z důvodu lepší aplikovatelnosti doménových politik.

Pokud stávající infrastruktura používá GPO je možno je do nové AD struktury v průběhu implementace naimportovat. Rovněž je důležité definovat a rozumně nastavit globální doménovou politiku, zejména ve vztahu k délce platnosti hesel, jejich komplexicitě a dalším parametrům, které budou ovlivňovat všechny uživatele.

Před vlastní implementací AD a nové infrastruktury bude vypracován a zadavatelem odsouhlasen plán implementace, kde budou detailně rozepsány jednotlivé instalační kroky a postupy, zohledněna rizika a dopady procesu implementace na jednotlivé uživatele.

Pozornost je potřeba věnovat zejména následujícím oblastem:

- Rozdělení FSMO rolí
- Nastavení Sites a replikací

- Instalace serverových rolí a fetures
- Příprava OU
- Příprava uživatelských skupin
- Administrátorská oprávnění
- Import uživatelských účtů
- Import GPO, tvorba nových GPO a GDP
- Definice zálohování a obnovy

7.3.2 DNSec

Domain Name System, známější pod svou zkratkou DNS, je internetový standard zahrnutý v TCP/IP. Slouží k překladu jmen objektů na IP adresy či jiné zdrojové záznamy (resource records). Jména objektů se označují jako doménová jména (domain name) a nejčastěji se jedná o jména hostitelů (hostname), jsou to alfanumerické řetězce, které jsou lépe zapamatovatelné než IP adresy. Nabízí i obrácenou funkci a to je překlad IP adres na jména objektů. K tomu se využívají tzv. PTR záznamy. Záznamy v DNS dnes existují nejen pro hostname, ale také pro řadu služeb a funkcionalitu Active Directory bez DNS je vlastně nemožná a Active Directory je na této službě závislá.

Tak, jako budou existovat řadiče domény, budou současně s těmito AD servery nasazena i služba DNS, která si bude záznamy mezi jednotlivými servery replikovat.

7.3.3 DHCP

Dynamic Host Configuration Protocol (DHCP) je název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru. DHCP server také zajišťuje zápis aktuálních údajů zařízení do DNS a je nedílnou součástí počítačové sítě.

Navrhujeme použít jeden centrální DHCP server s využitím Failover funkcionality služby v operačním systému Windows.

7.3.4 Radius

Mezi nejdůležitější vlastnosti patří jeho vysoká síťová bezpečnost, neboť transakce mezi klientem a RADIUS serverem je autentizována pomocí sdílení, které není nikdy posíláno přes síť. Pouze uživatelská hesla jsou přes síť zasílána šifrovaně. Uživatelská jména, účtování apod. můžou byt odposlechnuta třetí osobou, protože tyto data nejsou přenášena šifrovaně.

Postup autentizace je následující: uživatel vydá klientovi Požadavek na autentizaci, klient vytvoří Požadavek na přístup (Access Request) obsahující uživatelské jméno, heslo a ID portu, přes který je uživatel připojen.

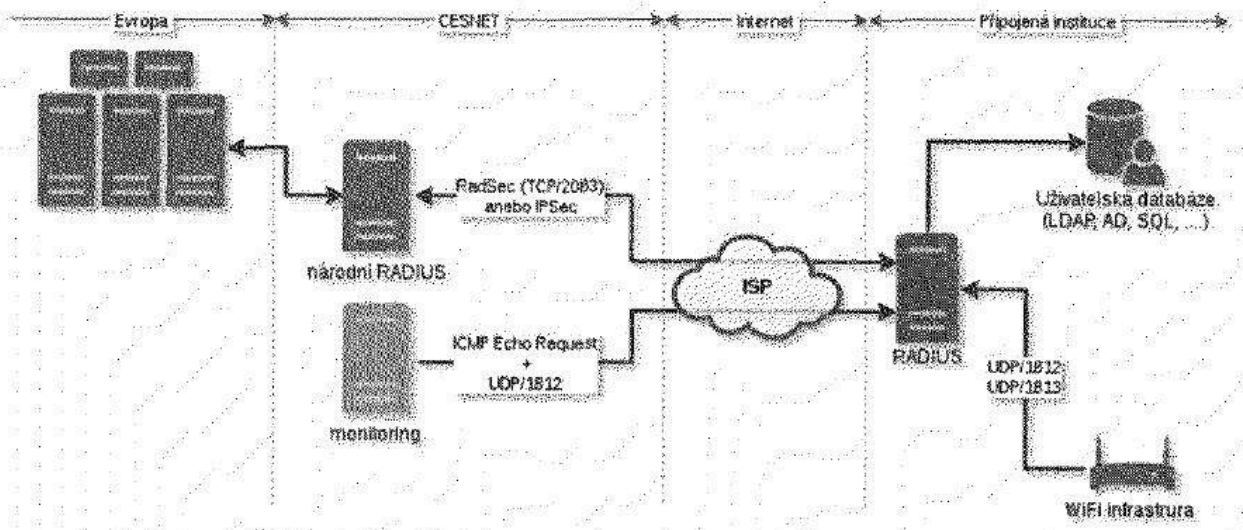
Požadavek na přístup je odeslán RADIUS serveru a čeká se na odpověď. Pokud nepřijde do určeného času (timeoutu) žádná odezva, Požadavek na přístup se opakuje, zpravidla 3 až 5 krát.

Pokud není splněna některá z podmínek, RADIUS server odešle Zamítnutí přístupu (Access Reject). Do datové oblasti paketu je dovoleno umístit maximálně textovou zprávu, která smí být zobrazena pomocí klienta uživateli. Žádné další atributy nejsou v odpovědi Access Reject povoleny.

Jestliže jsou všechny podmínky splněny, RADIUS server odešle Povolení přístupu (Access Accept), kde v datové oblasti paketu jsou uloženy všechny potřebné konfigurační informace (IP adresa, maska sítě, login uživatele a vše, co je potřeba předat požadované službě).

7.3.4.1 Propojení ERUDOAM

Do programu ERUDOAM bude škola zapojena v aktivním módu



Ve virtualizačním prostředí bude instalována linuxová appliance se službou FreeRADIUS v3. Tato služba bude zajišťovat propojení se sítí erudoam a bude sloužit pro ověřování návštěvnické WLAN. Propojení na síť erudoam je řešeno pomocí RADsec/IPsec protokolu a na appliance bude instalován CA serverový certifikát pro zabezpečení komunikace mezi školou a ERUDOAM infrastrukturou.

7.3.5 File Server

Další síťovou službou, která patří ke každé počítačové síti je sdílené úložiště dat postavené na službě File Sharing (sdílení souborů, resp. Souborový server), které slouží k ukládání všech typů souborů společnosti.

Sdílené úložiště by mělo obsahovat minimálně dva hlavní úložiště. První úložiště pro všechna společná data samozřejmě s patřičným nastavením přístupových práv do jednotlivých složek. Druhé úložiště pak pro ukládání uživatelských dat (soubory, profily, nastavení, ...). Důležitou součástí takovýchto úložišť je nastavení diskových kvót, kdy je tak možno i sledovat využití prostorů jednotlivými uživateli.

Hierarchii složek je nutné předem zvážit a přizpůsobit tak celkovému řízení práv na úrovni NTFS na základě skupin.

7.3.6 Tiskový server

Pro tisk bude využíván Windows server 2016. Tisk a sdílení souborů jsou základní sektory pro uživatele, skupiny, organizace v síti. Stejně jako v síti existuje velké množství tiskáren s různými odrůdami a existuje obrovský počet skupin uživatelů, kteří je potřebují používat. Jako správce byste měli vědět, jak nainstalovat a konfigurovat tiskové služby v systému Windows Server pro správu desítek nebo stovek tiskáren v síti. Vzhledem k tomu, že většina moderních tiskáren má síťovou síťovou kartu a adresy IP (Internet Protocol) mohou být přiřazeny k tiskárnám. Proto mohou všichni uživatelé prostřednictvím sítě přistupovat a používat je. Jedním z nejhmotnějších prvků v tiskových službách je sdružování tiskovin, pomocí něhož je k bazénu přidáno množství tiskáren. Když jedna provádí tiskovou úlohu, ostatní tiskárny provádějí další odeslané tiskové úlohy. Jelikož lze udělit prioritní přístup k tiskárně od 1 do 99. Pokud jsou na tiskovém serveru dvě tiskové úlohy, uživatel s vyšší prioritou dokončí úkol před jiným. Vše výše smiňované splňují tiskové služby v systému Windows Server 2016.

7.3.7 Terminálový server

Licenční server pro terminálové služby RDP - Windows server 2016 bude určený pro terminálové přístupy.

Terminálové služby Microsoft používají protokol RDP -- Remote Desktop Protocol, který je založen na protokolu T.120 a je definován pouze nad TCP/IP. RDP protokol obsahuje 64000 oddělených kanálů, které mohou přenášet různé typy dat (obraz, klávesnice, myš, zvuk, tisk, schránka apod.) . Protokol RDP podporuje i základní krytování přenášených dat – 56bit a 128bit RC4. Od Windows 2003 Serveru SP1 lze pro zabezpečení RDP protokolu použít i TLS. Terminálové služby standardně naslouchají na TCP portu 3389.

7.3.8 Informační systém

Bude instalováno zadavatelem

7.3.9 E-Learning

Bude instalováno zadavatelem

7.3.10 Backup SW NAKIVO Backup & Replication v7.3 pro VMware, Hyper-V, and AWS EC2

Rychlé, spolehlivé a cenově dostupné řešení pro zálohování, replikaci a obnovení soukromých a veřejných cloudových prostředí

7.3.10.1 Klíčové vlastnostina první pohled

- Instalace 1krát, snadno použitelné webové rozhraní
- Okamžité obnovení souboru
- Zálohování živých Hyper-V virtuálních počítačů založených na obrazu bez agentů
- Okamžité obnovení objektů Exchange
- Aplikace-vědomé, navždy-přírůstkové VM zálohování
- Okamžité obnovení objektů SQL
- Až 1 000 bodů obnovení GFS na jednu zálohu VM
- Okamžité obnovení objektů služby Active Directory
- Zabudovaná globální deduplikace a komprese dat
- Obnovení úplného VM na stejného nebo nového hostitele
- Vyloučení odkládacích souborů a oddílů
- Zkrácení protokolu SQL
- Zálohovat kopírování mimo a Azure / AWS mraky
- Zkrácení logu vým
- Automatické ověření zálohy
- Podpora sdílených svazků Hyper-V clusteru

7.3.10.2 zálohování Hyper-V

Nástroj Backup & Replication NAKIVO poskytuje nativní zálohování serverů Hyper-V Server 2016 a Hyper-V Server 2012 (R2).

Produkt může zálohovat živé spuštěné virtuální stroje Hyper-V bez nutnosti instalace agentů do VM nebo přerušení provozu VM. Aby byla zajištěna konzistentnost dat v aplikacích a databázích (například Exchange, Active Directory, SQL, SharePoint), může služba NAKIVO Backup & Replication používat režim zálohování, který závisí na aplikaci a který se spoléhá na technologii Microsoft VSS.
Výsledná záloha Hyper-V obsahuje všechny data VM a konfiguraci VM, takže můžete obnovit soubory OS, aplikační objekty a celý VM v přesně stejném stavu, jaký byl při zálohování.
Pro každou zálohu můžete uložit až 1 000 míst obnovy a každoročně, týdenně, měsíčně a každoročně je otáčet.

7.3.10.3 Zmenšení velikosti zálohy

Chcete-li snížit velikost zálohy instance AWS EC2, nástroj NAKIVO Backup & Replication automaticky přeskočí soubory a oddíly, které by jinak byly zpracovány, přeneseny a uloženy.

Kromě toho produkt automaticky deduplikuje všechny zálohy v celém zálohovém úložišti, takže v úložišti jsou uloženy pouze jedinečné datové bloky. Deduplicované bloky jsou komprimovány, a proto zabírají co nejmenší prostor. Společně tyto technologie snižování dat významně snižují zálohovací prostor obsazený zálohami instance AWS EC2.

7.3.10.4 Instant Granular Recovery

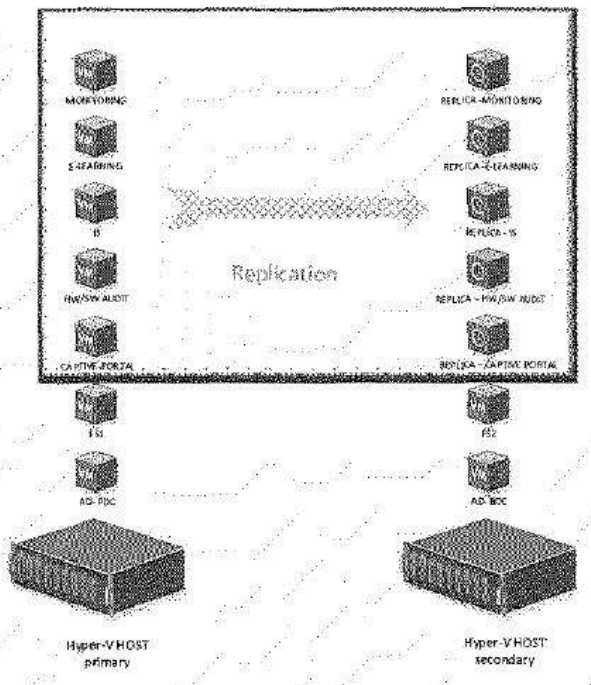
S nástrojem NAKIVO Backup & Replication můžete okamžitě obnovit soubory, objekty Microsoft Exchange, objekty Microsoft SQL Server a objekty Microsoft Active Directory přímo z deduplikovaných a komprimovaných záloh instancí AWS EC2.Můžete prohlížet, vyhledávat a obnovovat soubory a aplikační objekty ve webovém rozhraní produktu, aniž byste nejprve zotavili úplnou instanci AWS EC2.Tato funkce je čistě bez agentů a funguje mimo pro instance Windows i Linux.

7.3.10.5 Kopírování VM záloh mimo web a Cloud

VM zálohy mohou být ztraceny kdykoli a z různých důvodů, ať už kvůli selhání disku, škodlivému útoku nebo pouhému lidskému omylu.
Nejlepší způsob, jak chránit vaše zálohy VM a zajistit zálohy, je vytvořit záložní kopie a ukládat je mimo vaše datové středisko podle 3-2-1 zálohování osvědčených postupů, což naznačuje, že 3 kopie dat na 2 různých média, z nichž 1 je uloženo mimo provoz.
Snadno můžete přesunout záložní zařízení VM založené na technologii Synology mimo místo - dokonce i na místo, které nemá žádnou virtuální nebo serverovou infrastrukturu - a používat ho k udržení primárního nebo sekundárního zálohování VM.
Pokud dojde ke katastrofě, můžete ji obnovit buď v síti nebo přesunout zálohovací zařízení VM na požadované místo.
Pokud nemáte sekundární umístění, kde můžete bezpečně ukládat zálohy VM, vaše zálohovací zařízení VM postavené na zařízení Synology NAS může kopírovat zálohy do cloudu, například AWS nebo Azure.

7.4 Replikace

Virtuální servery nezbytné pro běh infrastruktury (Active Directory, Radius Server, File Server) budou provozovány na obou serverech. Ostatní virtuální servery budou replikovány na sekundární server pomocí Hyper-V replikace. V případě výpadku primárního serveru převezmou bez-výpadkově funkcionality kritické infrastruktury clusterované role AD, FS, NPS (radius). Zbytek virtuálních serveru se obnoví manuálně z replik provozovaných na sekundárním serveru.



V případě požadavků na vysokou dostupnost je možno provádět replikaci do MS AZURE cloudu.

7.5 Zálohovací síťové úložiště

7.5.1 Synology RS2818RP+ Rack

Škálovatelný server pro ukládání dat na požádání

RS2818RP + je ideální řešení pro malé a střední podniky s velkou flexibilitou, pokud jde o rozšiřitelnou paměťovou kapacitu, upgradovatelnou paměť a volitelnou vysokorychlostní podporu NIC. Je dokonale zapadá jako záložní cíl pro distribuované podniky, centralizovaný souborový server nebo záložní cíl pro pracovní stanice v rostoucím podnikání.

7.5.2 Jednoduché nasazení a transparentní správa

Řešení zálohování bez agenta centralizuje ochranu serverů Windows a Linux a minimalizuje nasazení i náklady na správu.

7.5.3 Zálohování bez agentů

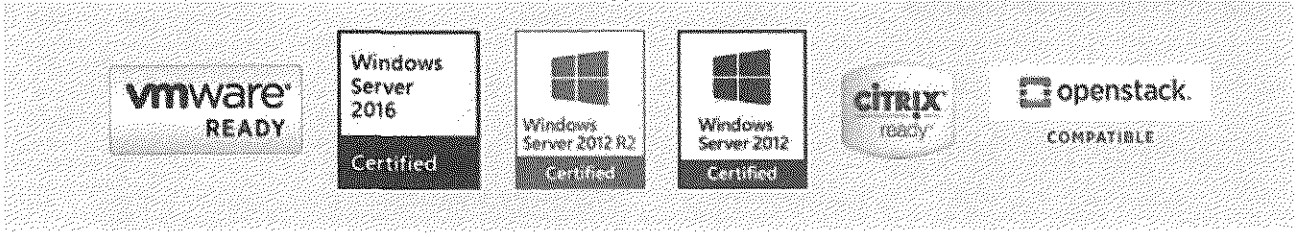
Zálohujte soubory denně, aniž byste museli instalovat složité a nákladné agenty na zdrojových serverech nebo se obávat, že ovlivní výkon klienta a kompatibilitu agentů.

7.5.4 Centralizované řízení

Sledujte všechny úkoly zálohování - zálohování systému Windows nebo Linux - z pohledu času a úlohy pomocí pokročilého nástroje histogramu na přehledové stránce a zjistěte abnormality na první pohled.

7.5.5 Plně certifikovaná řešení pro virtualizaci úložišť

Úložiště Synology iSCSI plně podporuje většinu virtualizačních řešení pro zvýšení efektivity práce s jednoduchým rozhraním pro správu. Integrace VMware vSphere 6 a VAAI pomáhá ukládat úložné operace a optimalizovat výpočetní efektivitu. Okamžitý přenos dat v systému Windows (ODX) zrychluje přenos dat a míru migrace. Podpora OpenStack Cinder přemění váš Synology NAS na blokovou komponentu.



7.5.6 Ochrana digitálních dat

Poradce pro zabezpečení

Analyzuje systémová nastavení, sílu hesla, předvolby sítě a odstraňuje případný malware.

AppArmor

Vylepšení na úrovni jádra, které blokuje škodlivé programy z přístupu k neoprávněným systémovým prostředkům.

AES 256 - bitové šifrování

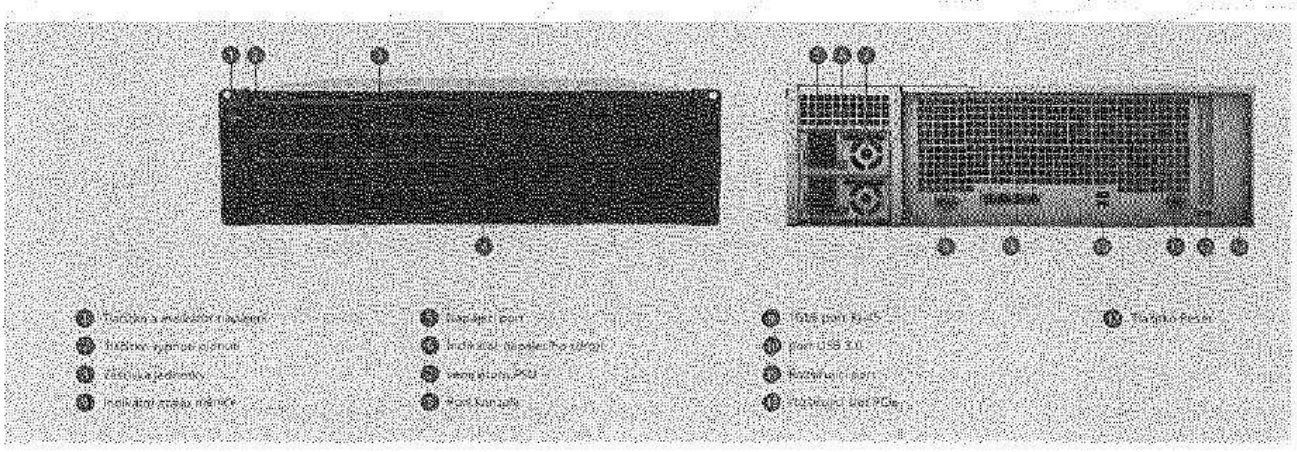
Šifrování sdílených složek a přenos dat v síti k uchování dat z neoprávněného přístupu.

Verifikace ve dvou krocích

Zabraňte ostatním při přihlášení k vašemu DSM vytvořením jednorázového hesla (OTP) v mobilním zařízení.

Úroveň důvěryhodnosti

Přizpůsobte úroveň důvěry v Balíčkovém centru, abyste zabránili instalaci balíčků z nedůvěryhodných zdrojů, chráníte váš NAS před neznámými nebo poškozenými soubory balíčků.



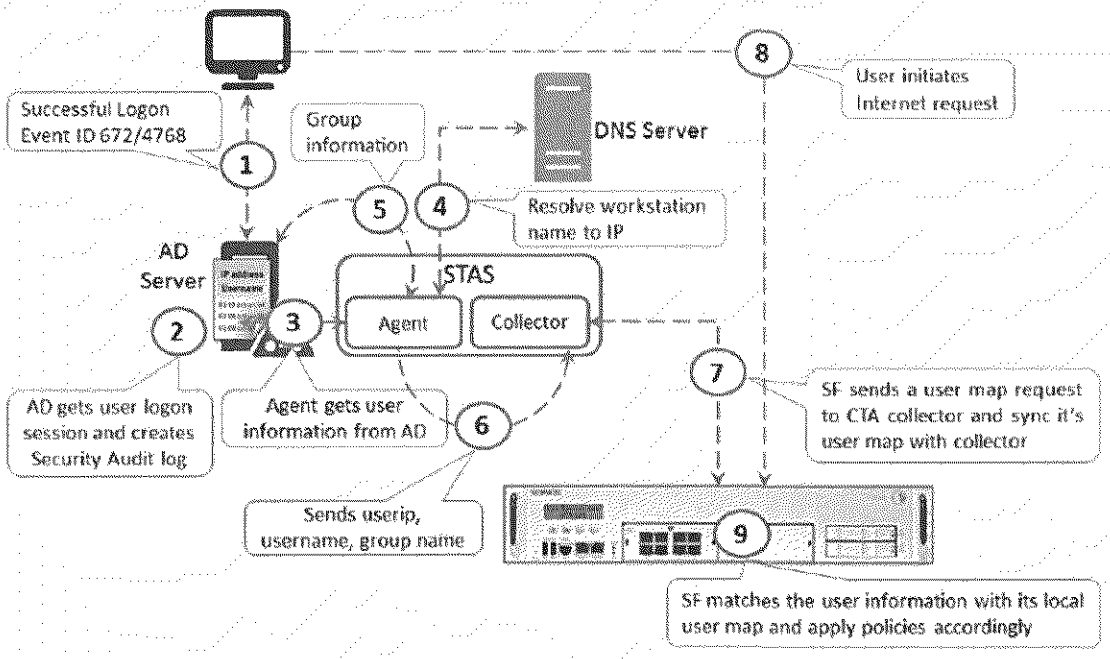
8 Přístup uživatelů do LAN

Autentizace SOPHOS Clientless Single Sign-On (SSO) umožňuje uživateli automaticky přidělovat síťové zdroje a aplikovat bezpečnostní politiky při přihlašování do systému Windows. To eliminuje potřebu vícenásobného přihlášení a odstraňuje potřebu instalovat klienty na každé pracovní stanici.

NGFW Sophos poskytuje jednotné přihlášení bez klientů ve formě Sophos Transparent Authentication Suite (STAS). Sada STAS zahrnuje:

- Agenta STAS - Sleduje požadavky na ověření uživatele a odesílá informace k ověřování STA Collector.
- Kolektor STAS - shromažďuje žádosti o ověření uživatelů od více agentů, zpracuje požadavek a poté je odešle do SF pro ověření.

8.1 Princip SSO Sophos



- Uživatel se přihlásí do řadiče domény služby Active Directory (AD) z libovolné pracovní stanice v síti LAN. AD ověřuje pověření uživatele
- Služba AD získává informace o relaci přihlášení uživatele a vytvoří protokol auditu zabezpečení. Po úspěšném ověření uživatele AD vytvoří událost s ID 4768 (Windows 2008 a vyšší).
- Agent pro monitorování serveru AD získává informace o relaci přihlašování uživatele z výše uvedených identifikátorů událostí.
- Agent dotazuje server DNS, aby vyřešil název pracovní stanice na adresu IP pomocí služby DNS nebo NetBIOS.
- Agent shromažďuje informace o skupině uživatele ze serveru AD.
- Agent předává současně uživatelské jméno, adresu IP a informace o skupině ke sběrateli přes výchozí port TCP (5566) současně.
- XG Firewall pošle žádost o mapování uživatelů na UDP port 6677 na kolektor a synchronizuje svou uživatelskou mapu s kolektorem. Kolektor odpovídá zasláním úspěšných aktualizací ověřování do brány XG Firewall na portu UDP 6060.
- Uživatel iniciuje požadavek na internet.
- XG Firewall odpovídá uživatelským informacím pomocí své místní mapy uživatelů a odpovídajícím způsobem používá zásady zabezpečení.

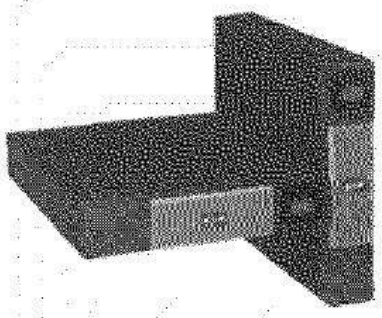
Na základě údajů agentu STA XG Firewall dotazuje server AD na určení členství ve skupině v závislosti na datech je přístup povolen nebo odmítnut. Uživatelé, kteří byli přihlášeni přímo do pracovní stanice (nebo místně), ale nejsou přihlášeni k doméně, nebudou ověřeni a považují se za neoprávněné uživatele. Pro uživatele, kteří nejsou přihlášeni do domény, bude pro ověření zobrazeno výzva pro ruční přihlášení.

9 Administrátorské přístupy

Přístup na aktivní prvky (LAN, WIFI, FIREWALL, NAS, MGMT serverů) za účelem jejich administrace bude řešen pomocí protokolu 802.1X (Radius). Funkci Radius serveru bude vykonávat role NPS (Network Policy Server) instalována na AD serverech. V kombinaci s AD bude zajišťovat administrátorský přístup definovaným uživatelům k vyhrazeným administračním rozhraním.

10 Rack UPS

Jako záložní zdroj bude použita UPS společnosti Eaton, konkrétně model Eaton 5PX 3000 VA (2U) Netpack.

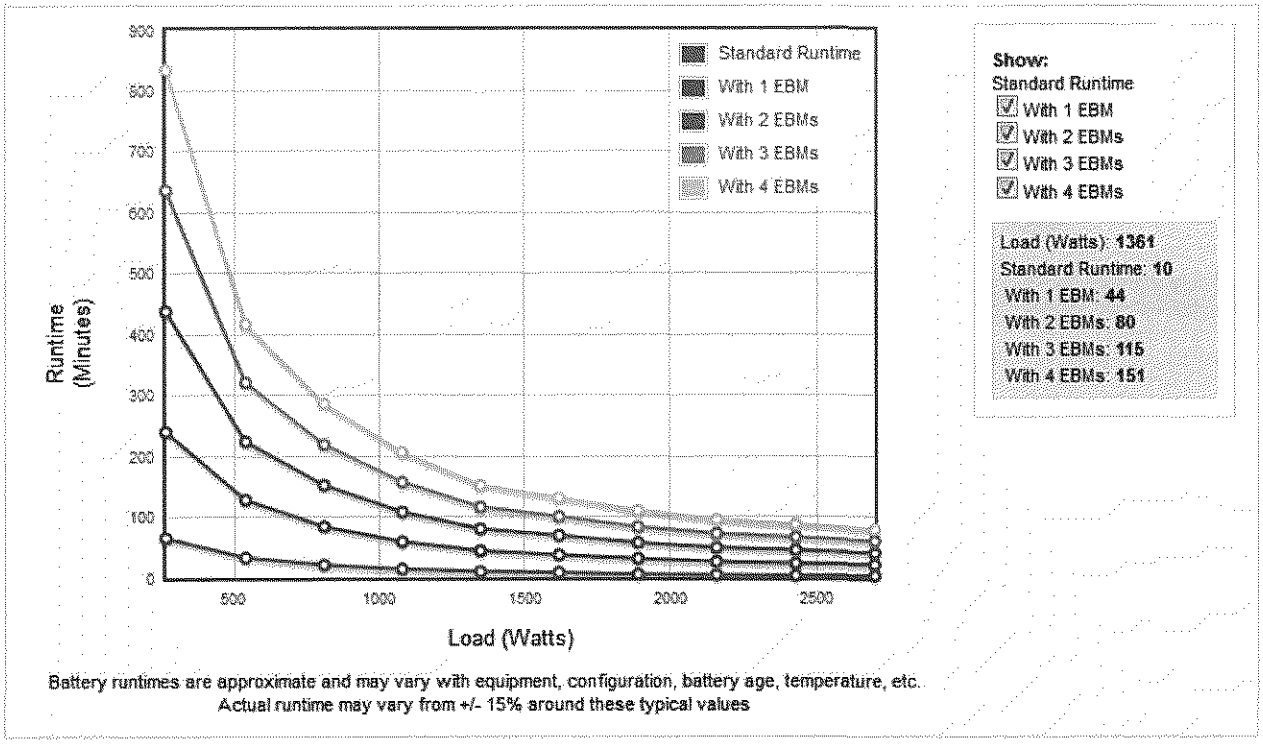


Všeobecné	
Topologie	Line-Interactive na vysokém kmitočtu (čistá sinusoida, regulace zvyšováním +snižováním)
Konfigurace	Tower/Rack výška 2U
Typové číslo	5PX3000IRTN
Zátěž (VA/W)	3000/2700
Rozměry V x Š xH, mm	86.2 x 441 x 647
Hmotnost kg	38.08
Záruční podmínky	3 roky na elektroniku, 2 roky na baterie
Obsah dodávky (dodává se s následujícími položkami)	1 univerzální UPS 2 IEC výstupní síťové šňůry CD se sadou programů Eaton Intelligent Power USB kabel Sériový kabel Minislot síťová karta (LAN adaptér) pro síťovou správu 2 podstavce pro věžovou (tower) montáž Šrouborák 2 úchyty pro montáž do 19" stojanu 2 univerzální lišty systém upevnění kabelových svazků montážní sada Bezpečnostní pokyny Návod Quick Start CD s uživatelskou příručkou v 10 jazycích

Vstupní	
Připojení vstupu	(1) IEC-320-C20 
Rozsah vstupního napětí bez nutnosti použít baterie	160V-294V (nastavitelné na 150V-294V)
Rozsah vstupního kmitočtu bez nutnosti použít baterie	47 až 70 Hz (soustava 50 Hz), 56,5 až 70 Hz (soustava 60 Hz), 40 Hz v režimu s nízkou citlivostí

Výstupní	
Napětí	230 V (+6/-10 %) -nastavitelné na 200V / 208V / 220V / 230V / 240V
Výstupní zásuvky	(8) IEC-320-C13 (1) IEC-320-C19  
Děkově ovládané zásuvky	2 skupiny - 2 x IEC C13 (10 A)
Výstupní kmitočet	50/60 Hz +/- 0,1 % (automatická detekce)

Baterie



Battery runtimes are approximate and may vary with equipment, configuration, battery age, temperature, etc.
Actual runtime may vary from +/- 15% around these typical values

Komunikační	
komunikační porty	1 USB port + 1 sériový port RS232 a relé kontakty (USB port a port RS232 nemohou být použity současně) + 1 blok svorkovnice pro dálkové zapnutí/vypnutí a dálkové odstavení
Komunikační zásuvné pozice	1 zásuvná pozice pro kartu NMC Minislot (součást dodávky)

Okolní prostředí / Homologace	
Akustický hluk	< 50 dBA
Provozních Teplota	0 až 40°C
Provedení - Bezpečnost - EMC	IEC/EN 62040-1-1 bezpečnost, IEC/EN 62040-2 EMC, IEC/EN 62040-3 provedení
Schválení	CE, CB report, TÜV

11 Klimatizace

Jako klimatizace bude použita sestava společnosti DAIKIN.

Vnitřní jednotka DAIKIN FTXB-C, venkovní jednotka DAIKIN RXB-C.

DAIKIN FTXB-C					FTXB35C2V1B
Skříň	Barva				Bílý
Rozměry	Jednotka		Výška	mm	283
			Šířka	mm	770
			Hloubka	mm	216
Hmotnost	Jednotka			kg	8
Ventilátor	Průtok vzduchu	Chlazení	Vysoké	m^3/min	9.3
			Nízký	m^3/min	6.1

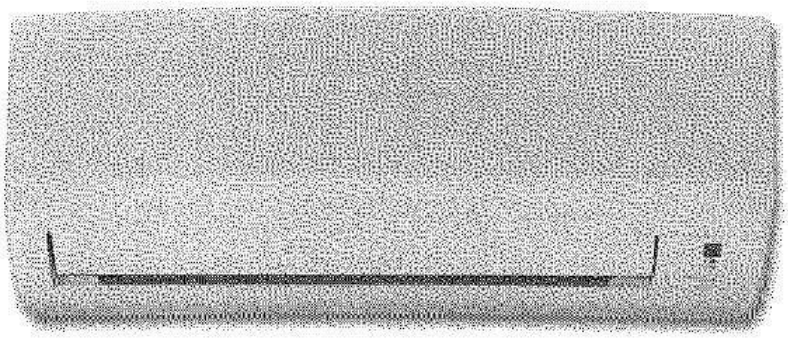
			Tichý provoz	m^3/min	4.9
		Vytápění	Vysoké	m^3/min	10.1
			Nízký	m^3/min	6.7
			Tichý provoz	m^3/min	5.7
			Nom.	m^3/min	7.7
		Vytápění	Jm.	m^3/min	8.4
Hladina akustického výkonu	Chlazení			dBA	58
	Vytápění			dBA	58
Hladina akustického tlaku	Chlazení		Vysoké	dBA	41
			Nízký	dBA	27
			Tichý provoz	dBA	23
	Vytápění		Vysoké	dBA	41
			Nízký	dBA	29
			Tichý provoz	dBA	26
			Jm.	dBA	34
	Vytápění		Jm.	dBA	35
Spoje potrubí	Kapalný		OD	mm	6.35
	Plyn		OD	mm	9.5
	Vypouštění				18
Standardní příslušenství	Položka				1
	Položka				1
	Položka				1
	Položka				2
	Položka				1
	Položka				1
	Položka				2
	Položka				2
Power supply	Name				V1
	Fáze				1~
	Frekvence			Hz	50
	Voltage			V	220-240

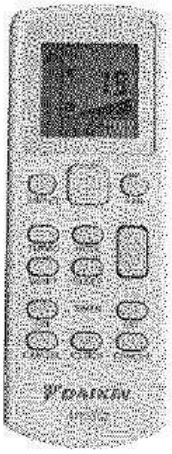
DAIKIN RXB-C					**RXB35C5V1B9**
Chladící výkon	Min./Jmen./Max.			kW	1,3 / 3,3 / 3,8
Topný výkon	Min./Jmen./Max.			kW	1,3 / 3,5 / 4,8
Rozměry	Jednotka		Výška	mm	550
			Šířka	mm	658
			Hloubka	mm	275
Hmotnost	Jednotka			kg	30

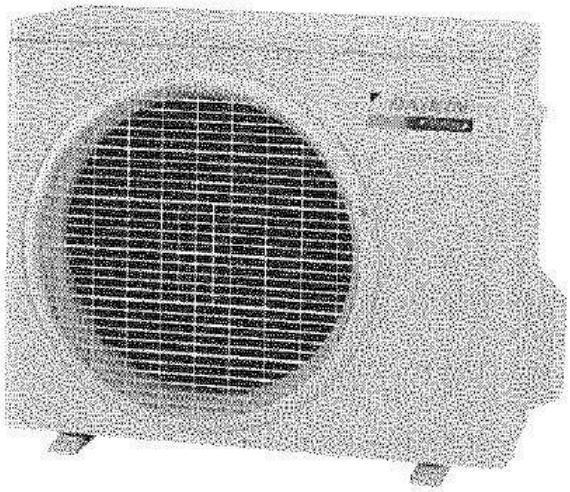
Kompresor	Typ				Hermeticky utěsněný rotační kompresor
Provozní rozsah	Chlazení	Okolí	Min.	°CDB	-10
			Max.	°CDB	46
	Vytápění	Okolí	Min.	° CWB	-15
			Max.	° CWB	18
Hladina akustického výkonu	Chlazení			dBA	62
	Vytápění			dBA	62
Hladina akustického tlaku	Chlazení		Vysoké	dBA	48
	Vytápění		Vysoké	dBA	48
Chladivo	Type				R-410A
	Náplň			kg	1.0
	Náplň			TCO2Eq	2.1
	GWP				2,087.5
Standardní příslušenství	Položka				1
	Položka				1
	Položka				1
	Položka				1
Power supply	Fáze				1~
	Frekvence			Hz	50
	Voltage			V	220-240

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR







DAIKIN

Příloha č. 2 – Specifikace provozních požadavků (požadavků na technickou podporu)

Zhotovitel poskytne technickou podporu po dobu 5 let od ukončení realizace díla. Zhotovitel garantuje u relevantních technologií podporu výrobce min. po dobu 5 let od ukončení realizace díla.

- Centrální router
  - Pravidelné bezpečnostní aktualizace systému, bezpečnostních databází a firmware
  - Záruka na dodaný HW a výměna na místě s opravou do 24h (24x7)
- Centrální bezpečnostní brána
  - Pravidelné bezpečnostní aktualizace systému, bezpečnostních databází
- Záruka na server
  - Záruka na dodaný HW a výměna na místě s opravou do 24h (24x7)
- Záruka na NAS
  - Záruka na dodaný HW a výměna na místě s opravou do 5 pracovních dnů (8x5)
- Profylaxe UPS
  - Roční kontrola UPS a baterií
  - Výměna baterií dle režimu doporučeného výrobcem (baterie musí být v ceně služby)
  - Záruka na provoz UPS po celou dobu udržitelnosti (5 let)
- Pravidelná údržba klimatizace
  - Roční kontrola dodané klimatizace
  - Výměna náplní či potřebných dílů dle režimu doporučeného výrobce (veškerý materiál musí být zahrnut v ceně služby)
  - Záruka na klimatizaci po celou dobu udržitelnosti (5 let)
- Maintenance - operační systém
  - Technická podpora výrobce minimálně v režimu (8x5)
  - Nárok na veškeré nové verze operačního systému vydané výrobce v době udržitelnosti (5 let)
- Maintenance - zálohovací a replikační SW
  - Technická podpora výrobce minimálně v režimu (8x5)
  - Nárok na veškeré nové verze operačního systému vydané výrobce v době udržitelnosti (5 let)
- Maintenance – SW pro audit a správu prostředků
  - Technická podpora výrobce minimálně v režimu (8x5)
  - Nárok na veškeré nové verze operačního systému vydané výrobce v době udržitelnosti
- Maintenance – LOG management
  - Technická podpora výrobce minimálně v režimu (8x5)
  - Nárok na veškeré nové verze SW vydané výrobce v době udržitelnosti (5 let)
  - Záruka na dodaný HW po celou dobu udržitelnost (5 let)
- Maintenance – Wi-Fi
  - Technická podpora výrobce minimálně v režimu (8x5)
  - Nárok na veškeré nové verze SW a firmware vydané výrobce v době udržitelnosti (5 let)
  - Záruka na dodaný HW po celou dobu udržitelnost (5 let)
- Technická podpora na instalované technologie
  - Měsíční kontrola logů a jejich vyhodnocení s předáním výsledného reportu
  - Měsíční kontrola a případná instalace opravných balíčků či bezpečnostních záplat na všechny systémy
  - Řešení hlášených havárií či nefunkcionalit systémů s dobou reakce do 24h
  - Údržba projektové dokumentace
  - Zaškolení na případné změny v systému

[redacted]

Příloha č. 3 – Minimální technické požadavky

Objednatel požaduje splnění následujících technických požadavků. Účastník v níže uvedené tabulce doplní v patřičném místě konkrétní typ výrobku (ů) a k nabídce přiloží jeho technické listy nebo jiné dokumenty prokazující naplnění minimálních technických požadavků včetně licenčních podmínek. Nesplnění byť jednoho z technických požadavků může vést k vyloučení.
Zhotovitel je povinen dodat typ výrobku, ke kterému se zavázal v této příloze nebo za stejnou cenu jeho novou vývojovou řadu za předpokladu, že splňuje nebo předčí všechny nabízené požadavky, bez nutnosti uzavírat dodatek k této smlouvě.

P. č.	Název a specifikace části	ks
1.	**Centrální síťový prvek - router a firewall**	2
	Sophos XG210 /active-pasive Failover/	
	HW appliance – ucelená jednotka v RACK provedení	ANO
	Záruka na HW 5 let v režimu Next Business Day	ANO
	Možnost provozu v konfiguraci cluster v případě zakoupení druhého node	ANO
	Rozhraní minimálně 4 x 1 Gbps Ethertnet, 1 x remote console, podpora agregace a redundance interface	ANO
	FW řešení podporující technologii stavového paketového filteru i aplikačních proxy bran firewallu	ANO
	Dedikovaný management port	ANO
	Podpora NAT / PAT	ANO
	Možnost řízení komunikace volitelně na sítových vrstvách L3 až L7	ANO
	Možnost řízení komunikace na úrovni jednotlivých aplikačních příkazů (aplikační proxy) alespoň pro protokoly: HTTP, SMTP, POP3, IMAP4, DNS, FTP, SIP, H.323, SQLNet	ANO
	Možnost HTTPS Inspekce (kontrola HTTPS, rozlamování TLS)	ANO
	Podpora VLAN	ANO
	Podpora IPV4 a IPv6, dual stack	ANO
	Podpora ICAP rozhraní	ANO
	Podpora SNMP	ANO
	QoS – řízení šířky pásma podle uživatele, portu i typu souboru	ANO
	Podpora autentizace (Kerberos, NTLM, LDAP, RADIUS)	ANO
	Zasílání NETFLOW v9 nebo IPFIX včetně informace o překladech IP adres se vzorkem max. 1:10 na min. jeden cíl	ANO
	Možnost doplnění VPN s dvou faktorovou SMS autentizaci pro uživatele	ANO
	Podpora Integrace s Microsoft Active Directory včetně řízení dle skupin uživatelů a podpory SSO tj. transparentní autentizace bez nutnosti ověřování mezi klientem a firewallem.	ANO
	Možnost ukončení TLS / SSL komunikace na FW s prováděním všech kontrol v šifrovaném provozu a to jak v provozu na server i klienta včetně rozšifrování a zašifrování spojení.	ANO

	Rozpoznávání a kontrola skutečných typů souborů v rámci HTTP komunikace (MIME Type) – nikoliv na základě deklarace klienta či serveru	ANO
	Možnost definice časové platnosti ACL pravidla, od-do	ANO
	Podpora Syslog, možnost exportu logu, možnost vzdáleného logování, podpora integrace do SIEM	ANO
	Autentizace uživatelů oproti MS Active directory, LDAP nebo lokální databáze uživatelů (protokol Kerberos nebo NTLM) bez nutnosti instalace klientského SW na stanici	ANO
	Podpora paralelní instalace více verzí firmware s možností okamžitého návratu k poslední verzi a libovolné přepínání	ANO
	Logování s podporou více úrovní a možností úplného záznamu komunikace na úroveň dump IP komunikace	ANO
	Zobrazování statistik a vyhodnocování provozu	ANO
	Záznamy provozu pro následný forenzní audit dle české jurisdikce	ANO
	Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let	ANO
	Kompletní instalace, konfigurace a zaškolení obsluhy.	ANO
	Dokumentace pro údržbu	ANO

P.č.	Název a specifikace části	Ks
2	**Centrální bezpečnostní brána** *Implementován v Sophos XG210 /active-pasive Failover/*	1
	Speciální HW nebo součást centrálního routeru.	ANO
	Jednotný management s centrálním síťovým prvkem (Router, firewall)	ANO
	Licence minimálně pro 450 žáků včetně podpory	ANO
	Modul Antivirus - licence minimálně pro 450 žáků včetně podpory	ANO
	Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let	ANO
	Česká databáze webových serverů	ANO
	Statistiky přístupu uživatelů k internetovým serverům	ANO
	Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu	ANO
	Zabezpečení přístupových protokolů (SSL/TLS), antivirová ochrana webových systémů	ANO
	Záruku na jakost kódu tzn. záruka odstranění bezpečnostní chyby do 10 dnů	ANO
	Podpora autentizace Kerberos a NTLM	ANO
	Výjimky z autentizace dle zdrojové nebo cílové IP adresy, nebo user agenta	ANO
	Podpora automatické detekce proxy pomocí WPAD	ANO
	Řízení přístupu na web dle kategorií obsahu	ANO
	Možnost definovat vlastní kategorií serverů	ANO
	Dostupná informace o úspěšnosti kategorizace pro webový provoz přes zařízení	ANO
	Politika přístupu definovaná dle času, kategorií, cílové URL, cílové IP adresy, uživatele, skupiny uživatel	ANO
	Definovatelné black/white listy pro jednotlivé uživatele nebo zdrojové IP adresy	ANO

	Kontrola obsahu HTTPS komunikace – HTTPS inspekce	ANO
	Možnost definovat důvěryhodné CA	ANO
	Výjimky z HTTPS inspekce na vybrané zdrojové IP adresy, servery nebo kategorie	ANO
	Integrovaná antivirová kontrola webového provozu (http, https)	ANO
	Blokování streamovaného obsahu (audio, video)	ANO
	Blokování rizikového tunelování (skype, teamwiever, tor, atd.)	ANO
	Možnost přeposílat vybraný provoz na nadřazenou proxy	ANO
	Jednoduché webové administrační rozhraní v českém jazyce	ANO
	Přehled o aktuálních informacích z provozu zařízení	ANO
	Více uživatelských účtů a rolí pro přístup k administračnímu rozhraní	ANO
	Administrační příručka v českém jazyce	ANO
	Nástroj pro testování změn v konfiguraci politiky přístupu na web před jejím uplatněním	ANO
	Jednoduchý nástroj pro prohledávání logovaných provozních záznamů	ANO
	Možnost nastavit dobu pro uchování logovaných provozních záznamů	ANO
	Podporu paralelní instalace více verzí firmware tzn. safe upgrade (možnost okamžitého návratu k poslední funkční verzi)	ANO
	Zařízení podporuje funkci cluster v případě zakoupení druhého boxu.	ANO
	Pokročilý reportovací nástroj dostupný z jednoho administračního rozhraní	ANO
	Synchronizace času pomocí NTP	ANO
	Interaktivní statistiky ve formátu HTML	ANO
	Periodicky generované statistiky provozu	ANO
	Generování statistik dle zadaných parametrů (filtrů)	ANO
	SSH přístup na konzoli HW zařízení	ANO
	Implementace a konfigurace	ANO
	Zaškolení obsluhy na konfiguraci webové brány	ANO

Úložiště aplikací a dokumentů

P. č.	Název a specifikace části	Ks
3	**Centrální server**	2
	DELL PowerEdge R540	
	Minimálně 2 procesory o celkovém výkonu minimálně 5934 bodů dle http://cpubenchmark.net/	ANO
	Minimální velikost paměti RAM 64 GB	ANO
	Rozhraní minimálně 2x - USB 2.0, 4x LAN (RJ-45)	ANO
	2 x SSD disk s minimální kapacitou 300GBANO	ANO
	2 x HDD v RAID 1 o kapacitě minimálně 6TB, rychlost otáček minimálně 7,2k	ANO
	Redundantní napájecí zdroj	ANO
	Management modul pro správu serveru	ANO

	4ks licence pro operační systém serveru (minimálně 8 instancí ve virtuálním prostředí). Minimální funkcionality: doménový řadič, DHCP server, DNS server, RADIUS server, souborový server, tiskový server, terminálový server. Možnost přiřazení stanic do domény s operačním systémem Windows 7 a vyšší. Možnost logování přihlášených uživatelů do domény.	ANO

P. č.	Název a specifikace části	ks
4	**Serverový rozvaděč s vybavením**	1
	Schrack DS426060-A	
	Formát 42U	ANO
	Minimální hloubka 1000 mm	ANO
	Minimální šířka 600 mm	ANO
	Větrák	ANO
	Perforované dveře	ANO
	Vybavení pro montáž serverů a aktivních prvků - montážní sady, vyvazovací panely	ANO

P. č.	Název a specifikace části	ks
5	**Klimatizace**	1
	DAIKIN RXB-C	
	Nástěnná klimatizace s plynulou regulací inverter včetně venkovní jednotky	ANO
	Min. 3,5 kW (chlazení)	ANO
	Rozvody chladiva	ANO
	Chladírenský a montážní materiál	ANO
	Dálkové ovládání	ANO
	Základní omyvatelné filtry	ANO
	Energetická třída min. A+	ANO
	Montáž včetně venkovní jednotky (2NP) a odvodu kondenzátu	ANO

P. č.	Název a specifikace části	ks
6.	**Rack UPS**	1
	Eaton 5PX 3000 VA (2U) Netpack	
	Minimální výkon 3 kVA	ANO
	Síťový management	ANO
	Rack UPS	ANO
	LCD display	ANO
	Minimálně 8 výstupních zásuvek	ANO

P. č.	Název a specifikace části	ks
7.	**Zálohovací síťové úložiště - 16 TB**	1

	Synology RS2818RP+ Rack	
	Provedení RACK	ANO
	Minimální disková kapacita v RAID 5 - 16TB	ANO
	Minimální celková rozšiřitelnost diskového úložiště - 100TB	ANO
	Minimální velikost RAM - 16GB	ANO
	Možnost měnit disky za chodu	ANO
	Minimální počet portů RJ-45 1GbE LAN port - 4 ks	ANO
	Redundantní napájení	ANO
	Podpora RAID - RAID 0, RAID 1,RAID 5,RAID 6, RAID 10	ANO
	Minimální počet souběžných připojení CIFS/AFP/FTP - 1000 připojení	ANO
	Minimální počet uživatelských účtů - 1000 účtů	ANO
	Integrace s Windows ACL (Access Control List)	ANO
	Podpora virtualizace - VMware vSphere, Citrix XenServer, OpenStack, Hyper-V	ANO
	Podpora - VPN server, video server, media server	ANO
	Centrální management	ANO

P. č.	Název a specifikace části	ks
8.	**Software pro zálohování a replikaci**	1
	NAKIVO Backup & Replication v7.3	
	Licence na zálohovací systém pro zálohování virtuální infrastruktury serverů a dat s možností i „bezagentového" zálohování celých virtuálních serverů i jednotlivých dat uvnitř virtuálních serverů	ANO
	Replikace virtuálních serverů do druhé lokality s oknem maximálně 15 minut	ANO
	Provoz zálohovacího systému ve virtuální appliance či na volně dostupném OS bez nutnosti kupovat další licenci na operační systém	ANO
	Podpora zálohování Microsoft Windows serverů (minimálně 2008 a vyšší), podpora Linux serverů	ANO
	Podpora archivace na externí disk nebo do cloudu NAKIVO Backup & Replication v7.3	ANO
	Podpora deduplikace dat v rámci celého cílového úložiště	ANO
	Přímý přístup k datům v záloze	ANO

P. č.	Název a specifikace části	ks
9.	**HW a SW pro vyhodnocování a sběr logů ze síťových prvků a virtuálních serverů**	1
	DELL PowerEdge R440 + SW Siemonster	
	HW appliance	ANO

	Minimálně licence na 300 zařízení nebo neomezený počet zdrojů pro zpracování logů	ANO
	Minimální počet zpracovaných událostí - 1000 událostí/s	ANO
	Zpracování logů z dodané bezpečnostní brány a centrálního routeru. Dohledatelnost vazeb veřejného provozu k vnitřnímu zařízení v síti.	ANO
	Zpracování logů ze současných aktivních prvků. Dohledatelnost provozu v rámci vnitřní sítě. Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ)	ANO
	Zpracování logů z implementovaného Microsoft Active Directory. Dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)	ANO
	Systém pro sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců	ANO
	Detekce nelegitimního provozu a síťových anomálií (vyhodnocení v rámci sesbíraných logů z bezpečnostní brány)	ANO

P. č.	Název a specifikace části	ks
	SW pro audit a správu ICT prostředků	**1**
	AW Caesar	
	Podpora mobilních zařízení Android, iOS	ANO
	Podpora PC a NB s OS Windows a Linux	ANO
	Automatické objevování zařízení	ANO
	Audit hardware, vč. možnosti přidání zadání zařízení mimo sledované prostředky	ANO
10.	Načítání informací o HW pomocí SNMP	ANO
	Možnost auditu softwaru a zakoupených licencí na sledovaných PC	ANO
	Licenční pokrytí 190 zařízení	ANO
	Víceúrovňová správa uživatelů (student, učitel, it technik)	ANO
	Klient pro vzdálené sledování prostředků	ANO
	Možnost vytváření reportů pro sledované prostředky	ANO
	Aktivní upozorňování příslušných osob, především správce na změny v hw/sw u sledovaných stanic	ANO

P. č.	Název a specifikace části	ks
	Instalace	**1**
	Implementace Microsoft RADIUS serveru pro autorizaci uživatelů a zařízení do sítě	ANO
	Instalace rozvaděče a zapojení do stávající síťové infrastruktury	ANO
11.	Instalační a konfigurační práce na zapojení serveru a serverového clusteru	ANO
	Instalace a konfigurace Active Directory clusteru a DNSSEC resolveru	ANO
	Implementace SW pro sběr a vyhodnocování logů	ANO
	Implementace zálohovacího SW a úložiště	ANO
	Dokumentace a zaškolení obsluhy na údržbu systému	ANO

Navýšení Wi-Fi sítě

P. č.	Název a specifikace části	ks
AP-	**Wi-Fi prvky (AP)**	19
	Sophos AP100	
	Podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...	ANO
	Podpora mechanismu izolace klientů	ANO
	Minimální počet připojených zařízení na AP – 30ks	ANO
	Centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)	ANO
	Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)	ANO
	Podpora standardu minimálně IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz	ANO
	Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu	ANO
	Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů	ANO
	Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let	ANO
	Kompletní instalace, konfigurace a zaškolení obsluhy na správu počítačové sítě	ANO
	Dokumentace pro údržbu	ANO
	Montáž Wi-Fi zařízení a dotažení kabelů k Wi-Fi, zalištování	ANO
	Konfigurace Wi-Fi sítě a zaškolení obsluhy	ANO

P. č.	Název a specifikace části	ks
13.	**Centrální řídící prvek Wi-Fi sítě**	2
	Implementován v Sophos XG210 + IAC-BOX	
	WLAN kontroler pro min. 30x AP	ANO
	podpora L2/L3 fast roamingu klientů	ANO
	podpora Bridge i Routing mode - min. 2x WAN 1G porty a min. 8x LAN 1G	ANO
	Integrovaný accounting a billing uživatelů - min. 1000 lokálních účtů	ANO
	podpora autorizace uživatelů vůči externím serverům přes Radius, LDAP, NT domain, SIP, POP3	ANO
	podpora min. 8x rozdílných captive portálů včetně rozdílného designu a služeb	ANO
	podpora Captive portálů optimalizovaných pro mobilní klienty	ANO
	podpora loginu přes QR kódy	ANO
	podpora loginu přes sociální sítě, SMS i email	ANO
	integrované odchytávání paketů pro analýzu dat. provozu	ANO
	automatická podpora rozpoznání AP a jeho konfigurace	ANO

	podpora správy AP na LAN i WAN portech (L2 i L3)	ANO
	podpora AP load balancing	ANO
	podpora detailního nastavení služeb dle času, místa, uživatelské role, přenesených dat apod.	ANO
	integrovaný firewall	ANO
	DHCP sever i relay	ANO
	NAT	ANO
	WAN port failover a load balancing	ANO
	static routing, RIP, OSPF	ANO
	detailní logování přímo ve WLAN kontroleru - UAMD log, firewall, DHCP, AP, user log, traffic log, ...	ANO

Celková dokumentace a předání projektu

P. č.	Název a specifikace části	ks
	Dokumentace a ověření	**1**
	Předání kompletní dokumentace k instalovaným komponentům v rámci projektu a způsob jejich údržby	ANO
	Aktualizovaná kompletní výkresová dokumentace ke strukturované kabeláži, včetně popsaných zásuvek a měřících protokolů.	ANO
	Na základě realizovaného projektu zpracuje zásady využívání ICT a přístupu k síti do vnitřních předpisů školy.	ANO
14.	Zhotovitel provede komplexní kontrolu celé sítě na základě doporučení http://www.dotaceeu.cz/getmedia/36c80ac4-db39-48f4-a730-4a4bea8f65aa/Standard-konektivity_overeni-a-kontrola_cerven-2017_final.pdf a předá veškeré protokoly o kontrole.	ANO
	Test výpadku napájení elektrické energie. Servery musí být funkční minimálně po dobu 10 minut a následně se regulérně ukončit	ANO
	Test obnovy libovolného virtuálního serveru a test obnovy dat	ANO
	Zhotovitel provede komplexní zaškolení obsluhy na provoz a údržbu sítě, včetně vyhodnocování logů, práci s Webovým filtrem, přidávání a rušení zařízení či uživatelů v rámci sítě, apod.	ANO

Příloha č. 4 – Položkový rozpočet

	Cena celkem bez DPH	Cena celkem s DPH
Cena za I. fázi (realizační a implementační)	1 377 595 Kč	1 666 889,95 Kč
Cena za II. fázi (provozní)	622 527 Kč	753 257,67 Kč
Celkem	2 000 122 Kč	2 420 147,62 Kč

Název položky	Cena za kus bez DPH	ks	Cena celkem bez DPH	Cena celkem s DPH
I. Fáze – realizační a implementační				
Centrální router				
Centrální router pro připojení včetně IDS a IPS	132 531	1	132 531 Kč	160362,51 Kč
Instalace a konfigurace centrálního routeru, zaškolení	26 100	1	26100 Kč	31 581,00 Kč
Bezpečnostní webová brána				
Licence do 450 žáků první rok	87 542	1	87 542 Kč	105 925,96 Kč
Implementace a konfigurace bezpečnostní brány	10 440	1	10 440 Kč	12 632,30 Kč
Zaškolení obsluhy na konfiguraci webové brány	5 220	1	5 220 Kč	6 316,15 Kč
Centrální server -uložiště aplikací a dokumentů				
Centrální server rack, 2x8C, 64GB RAM, 2x300GB SSD, 2x6TB HDD 7,2k, centrální správa	81 274	2	162 548 Kč	196 682,28 Kč
Serverový rozvaděč s vybavením, větrák	26 976	1	26 976 Kč	32 640,89 Kč
Klimatizace včetně instalace	45 190	1	45 190 Kč	54 680,46 Kč
UPS 3kVA, management	40 118	1	40 118 Kč	48 542,86 Kč
Zálohovací síťové úložiště - 16TB	92 225	1	92 225 Kč	111 592,78 Kč
SW pro zálohování a replikaci	58 699	1	58 699 Kč	71 026,02 Kč
Licence pro operační systém serveru	17696	4		

			70 784 Kč	85 647,46 Kč
SW pro vyhodnocování a sběr logů ze síťových prvků a virtuálních serverů	150 443	1	150 443 Kč	182 035,73 Kč
SW pro audit a správu ICT prostředků	25 671	1	25 671 Kč	31 061,85 Kč
Implementace Microsoft RADIUS serveru pro autorizaci uživatelů a zařízení do sítě	5 220	1	5 220 Kč	6 316,15 Kč
Instalace rozvaděče a zapojení do stávající síťové infrastruktury	10 440	1	10 440 Kč	12 632,30 Kč
Instalační a konfigurační práce na zapojení serveru a serverového clusteru	10 440	1	10 440 Kč	12 632,30 Kč
Instalace a konfigurace Active Directory clusteru a DNSSEC resolveru	10 440	1	10 440 Kč	12 632,30 Kč
Implementace SW pro sběr a vyhodnocování logů	26 100	1	26 100 Kč	31 580,76 Kč
Implementace zálohovacího SW a úložiště	10 440	1	10 440 Kč	12 632,30 Kč
Dokumentace a zaškolení obsluhy na údržbu systému	10 440	1	10 440 Kč	12 632,30 Kč
WI-FI - aktivní síťové prvky				
Wi-Fi AP - 2 rádia, kapacita min. 30 uživatelů	12 326	19	234 194 Kč	283 373,13 Kč
Centrální řídící prvek Wi-Fi sítě	42085	2	84 170 Kč	101 845,15 Kč
Montáž Wi-Fi zařízení, zapojení do sítě LAN	576	19	10 944 Kč	13 251,64 Kč
Dotažení nové dvojzásuvky 5.1.04 do učebny 102 v budově F z rozvaděče DR-5 (dvoupozicová datová zásuvka 2x RJ45 STP (1ks), instalační kabel CAT5E FTP PVC (40 m) včetně instalace a montáže - z jedné pozice dojde k napojení Wi-Fi)	3 914	1	3 914 Kč	4 735,72 Kč
Napojení Wi-Fi AP ze zásuvky 5.1.03 v budově F (zalištování)	2 876	1	2 876 Kč	3 480,30 Kč
Konfigurace Wi-Fi sítě a zaškolení obsluhy	7830	2	15660 Kč	18 948,45 Kč
ICT do řádu školy				
Zapracování ICT do řádu školy		1		

	7 830		7 830 Kč	9 474,23 Kč

II. fáze – provozní (celkem za 5 let)				
Centrální router	52 119	1	52 119 Kč	63 063,99 Kč
Centrální bezpečnostní brána	92 751	1	92 751 Kč	112 228,71 Kč
Záruka server	69 169	1	69 169 Kč	83 694,49 Kč
Záruka NAS	5 764	1	5 764 Kč	6 974,44 Kč
Profylaxe UPS	34 585	1	34 585 Kč	41 847,85 Kč
Pravidelná údržba klimatizace	40 349	1	40 349 Kč	48 822,29 Kč
Maintenance Operační systém	40 349	1	40 349 Kč	48 822,29 Kč
Maintenance zálohovací a replikační SW	5000	1	5000 Kč	6050 Kč
Maintenance na SW pro audit a správu prostředků	40 349	1	40 349 Kč	48 822,29 Kč
Maintenance na LOG management	103 754	1	103 754 Kč	125 542,34 Kč
Maintenance Wi-Fi	69 169	1	69 169 Kč	83 694,49 Kč
Technická podpora na instalované technologie	69 169	1	69 169 Kč	83 694,49 Kč

[redacted]

[redacted]