

Příloha č. 6: Nabídka Zhotovitele



Předmět nabídky:

„Bezpečné síťové prostředí“

Nabídka pro:

Hlavní město Praha

Datum publikace: 27. 06. 2018
Status: Originál

Nabídka pro: Hlavní město Praha
Mariánské nám. 2, 110 01 Praha 1
110 00 Praha 1 – Nové Město

K rukám:

Uchazeč:
Kontaktní spojení:

Vypracovali:

Schválil:

Dne:

Zadávací lhůta:

Počet stránek:

Corpus Solutions, a.s.

Corpus Solutions, a.s.

27. 06. 2018

Zadávací lhůta není stanovena

190

Omezující podmínky pro zveřejnění a použití:

Tento dokument obsahuje informace důvěrného charakteru a je určen výhradně pověřeným pracovníkům Magistrátu hlavního města Prahy a osobám pověřeným výkonem zadavatelských činností, jako takový nesmí být bez předchozího souhlasu Corpus Solutions a.s. kopírován, předán či jinak zpřístupněn třetí fyzické nebo právnické osobě, ani použit pro jiné účely než je posouzení uchazečů ve výběrovém řízení.

Upozornění:

Všechny známky a názvy produktů uvedené v tomto materiálu jsou nebo mohou být registrované obchodní značky, obchodní známky nebo ochranné známky jejich vlastníků.

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je zapsána u rejdičkového soudu
v Praze pod spisovou značkou B5936

Strana 1/190

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je zapsána u rejdičkového soudu
v Praze pod spisovou značkou B5936

Strana 2/190

Poděkování

Velice si vážíme možnosti, že naše společnost Corpus Solutions a.s. může nabídnout své služby právě Magistrátu hlavního města Prahy.

Pevně věříme, že námi navržené řešení a zvolený přístup odpovídají Vaším představám a požadavkům.

S úctou za společnost Corpus Solutions a.s.

předseda představenstva

I Identifikační údaje dodavatele

Obchodní jméno: Corpus Solutions a.s.
Sídlo společnosti: Štětčova 1638/18, 147 00 Praha 4
Právní forma společnosti: Akciová společnost
Statutární orgán: vedená u Městského soudu v Praze pod spisovou značkou B. 5936
Představenstvo:

Založení společnosti: 1992

Kontakt na osobu oprávněnou zastupovat dodavatele

Bankovní spojení

IČ

DIČ

Telefon

ID Datové schránky

Předmět podnikání

25764616

CZ25764616

(+420) 241 020 333

Zchpac2

Výroba, obchod a služby neuvedené v přílohách I až 3 živnostenského zákona

Zprostředkování obchodu a služeb

Velkoobchod a maloobchod

Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály

Pronájem a půjčování věcí movitých

Poradenská a konzultační činnost, zpracování odborných studií a posudků

Příprava a vypracování technických návrhů, grafické a kresličské práce

Testování, měření, analýzy a kontroly

Reklamní činnost, marketing, mediální zastoupení

Služby v oblasti administrativní správy a služby organizačně hospodářské povahy

Mimoškolní výchova a vzdělávání, pořádání kurzů, školení, včetně lektorské činnosti

Poskytování technických služeb

Výroba, obchod a služby jinde nezařazené

1,02 mil. Kč

Základní jmění

www

www.corpus.cz

Společnost Corpus Solutions a.s. (založena 1992) je předním dodavatelem služeb a technologií v oblasti zabezpečení informačních systémů. V projektech kombinujeme znalosti teoretické základny (doloženo certifikáty pracovníků) s praktickými zkušenostmi získanými při realizaci technologických projektů.

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je zapsána u rejdičkového soudu
v Praze pod spisovou značkou B5936

Strana 3/190

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je zapsána u rejdičkového soudu
v Praze pod spisovou značkou B5936

Strana 4/190

2 Obsah

1	Identifikační údaje dodavatele	4
2	Obsah	5
3	Příloha č. 3 - Nabídková cena dle článku 5 zadávací dokumentace	6
4	Závazný návrh smlouvy	6
5	Další doklady a dokumenty	186
6	Informace o celkovém počtu listů nabídky	190

3 Příloha č. 3 - Nabídková cena dle článku 5 zadávací dokumentace

Příloha č. 3 - Nabídková cena

Položka č.	Dílčí plnění	Množství (ks)	Cena za ks v Kč bez DPH	Cena v Kč bez DPH
1	Vypracování Detailního návrhu řešení	1	500 000,00 Kč	500 000,00 Kč
2	Dodávka technologií pro Bezpečné síťové prostředí	1	87 120 198,31 Kč	87 120 198,31 Kč
3	Instalace a implementace v jednotlivých lokalitách	1	10 000 000,00 Kč	10 000 000,00 Kč
4	Služby úpravy konfigurací současných bezpečnostních technologií	1	5 100 000,00 Kč	5 100 000,00 Kč
5	Služby záruky a podpora výrobce technologie	1	26 029 801,69 Kč	26 029 801,69 Kč
6	Služby školení zadavatele a servisní podpory spojené s provozem technologie	1	1 100 000,00 Kč	1 100 000,00 Kč
7	Cena za 1 člověkodenní poskytování dalších odborných služeb**	800	12 500,00 Kč	10 000 000,00 Kč
Cena celkem v Kč bez DPH				139 850 000,00 Kč

** Jedná se o modelový počet 800 člověkodenní, nikoliv maximální objem

V Praze dne 27. 06. 2018



Člen představenstva
Corpus Solutions a.s.



Corpus Solutions a.s.
Sídlo: 163 00 Praha 4
IČ: 25764616

Corpus Solutions a.s.
Sídlo: 163 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudu v Praze pod spisovou značkou B5936
Strana 5/190

Corpus Solutions a.s.
Sídlo: 163 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudu v Praze pod spisovou značkou B5936
Strana 6/190

4 Závazný návrh smlouvy

SMLOUVA O DÍLO

Číslo smlouvy Objednatel: _____

Číslo smlouvy Zhotovitel: _____

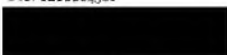
uzavřená níže uvedeného dne, měsíce a roku podle ustanovení § 2586 a n. zákona č. 89/2012 Sb., občanský zákoník (dále jen „**Občanský zákoník**“), „**obč. zák.**“ nebo „**o.z.**“) a na základě zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů; (dále jen „**Smlouva**“), mezi níže uvedenými smluvními stranami:

Hlavní město Praha

se sídlem Mariánské náměstí 2/2, 110 01 Praha 1

zastoupené [redacted] ředitelem odboru informatiky Magistrátu hl. m. Prahy

IČO: 00064581
DIČ: CZ00064581



(dále jen „**Objednatel**“)

a

Corpus Solutions a.s.

se sídlem: Štětčkova 163/18, 140 00 Praha 4

jejímž jménem jedná/zastoupená [redacted] předseda představenstva

IČO: 25764616
DIČ: CZ25764616

Bankovní spojení: [redacted]
Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 5936

(dále jen „**Zhotovitel**“)

(Objednatel a Zhotovitel společně dále jen „**Smluvní strany**“ nebo jednotlivě též jen „**Smluvní strana**“)

ÚVODNÍ USTANOVENÍ

Objednatel dne 21. 6. 2018 odeslal v rámci „ČÁSTI 1 Dodávky HW zařízení a standardního SW“ dynamického nákupního systému s názvem „Dodávky HW zařízení, standardního SW a odborných služeb technického poradenství“ (dále jen „**DNS**“) výzvu k podání nabídek na veřejnou zakázku s názvem „**Bezpečné síťové prostředí**“ (dále jen „**Veřejná zakázka**“). Nabídka Zhotovitele byla na základě kritéria ekonomické výhodnosti nabídky vybrána jako nejvhodnější, proto Smluvní strany uzavírají tuto Smlouvu.

1 PŘEDMĚT SMLOUVY

1.1 Předmětem plnění této Smlouvy je povinnost Zhotovitele provést pro Objednatel dílo spočívající v dodání, instalaci a implementaci technologií i služeb bezpečného síťového prostředí (dále jen „**Dílo**“). Předmětem Díla podle této Smlouvy jsou zejména následující dílčí plnění:

(a) Vypracování projektu detailního návrhu řešení (dále jen „**Detailní návrh řešení**“) a dodání veškerého softwarového a hardwarového vybavení potřebného k provozování všech požadovaných součástí včetně softwarových licencí.

(b) Dodávka odborných služeb instalace a implementace do prostředí Objednatel, poskytnutí servisní podpory a záruk k dodaným technologiím, jakož i zaškolení administrátorů systémů a zpracování dokumentace.

(c) Další odborné služby nezahrnuté pod písm. a) či b) odst. 1.1 této Smlouvy, které budou hrazeny na základě skutečně provedené práce vyjádřené v člověkodnech.

1.2 Dílo podle této Smlouvy zahrnuje provedení prací a/nebo poskytnutí služeb, které obvykle s provedením Díla souvisí, a jejichž provedení je nutné za účelem řádného provedení Díla a jeho funkčnosti ve smyslu **Přílohy č. 1**, která je nedílnou součástí této Smlouvy, bez ohledu na to, zda jsou v této Smlouvě uvedeny či nikoliv.

1.3 Podrobná specifikace vlastností požadovaného Díla, jakož i závazné postupy pro implementaci a vedení projektu jsou uvedeny v **Příloze č. 1**, která je nedílnou součástí této Smlouvy.

2 TERMÍN A MÍSTO PLNĚNÍ

2.1 Termínem zahájení plnění Díla je den účinnosti této Smlouvy.

2.2 Zhotovitel je povinen provést Dílo v termínech uvedených v harmonogramu plnění v **Příloze č. 4** a v Detailním návrhu řešení, případně dle udělených Pokynů Objednatel.

Corpus Solutions a.s.
Sídlo: 163 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudu v Praze pod spisovou značkou B5936
Strana 7/190

Corpus Solutions a.s.
Sídlo: 163 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudu v Praze pod spisovou značkou B5936
Strana 8/190

2.3 Místem plnění Díla je sídlo Objednatel, sídlo Zhotovitele, a případně jiná místa na území hl. m. Prahy určená Objednatel.

3 CENA

- 3.1 Celková cena za Dílo činí:
139 850 000 Kč (slovy: dvacet devět milionů tři sta šedesát osm tisíc pět set korun českých korun českých), bez zákonom stanovené daně z přidané hodnoty (dále jen „DPH“);
DPH činí **29 368 500 Kč (slovy: dvacet devět milionů tři sta šedesát osm tisíc pět set korun českých korun českých);**
169 218 500 Kč (slovy: jedno sto šedesát devět milionů dvě stě osmnáct tisíc pět set), včetně DPH;
(dále jen „Cena“). Podrobná specifikace Ceny je obsažena v **Příloze č. 5** této Smlouvy.
- 3.2 Cena je cenou nejvýše přípustnou, úplnou a závaznou, a Zhotovitel prohlašuje, že plně pokrývá všechny jeho náklady spojené s provedením Díla podle této Smlouvy. Cena uvedená v čl. 3.1. díle této Smlouvy zahrnuje rovněž cenu za zajištění soudnosti třetích osob dle čl. 7.14 této Smlouvy a cenu za práva k Dílu dle čl. 14 této Smlouvy.
- 3.3 Smluvní strany vylučují použití ustanovení § 2611 obč. zák.

4 PŘEDÁNÍ A PŘEVZETÍ DÍLA, UDĚLENÍ POKYNU K PLNĚNÍ

- 4.1 Dílčí celek Díla dle čl. 1.1 bod (a) této Smlouvy – Detailní návrh řešení obsahující alespoň náležitosti dle čl. 4.1 **Přílohy č. 1** zadávací dokumentace Veřejné zakázky Zhotovitel předá Objednateli k připomínkám nejprve v elektronické podobě ve formátu MS Word (verze MS Word 2010 a vyšší) a v termínu dle harmonogramu plnění, který tvoří **Přílohu č. 4** této Smlouvy. Objednatel zpracovává své připomínky formou revizí v termínu 10 pracovních dnů ode dne obdržení tohoto dílčího celku Díla, nedohodnou-li se oprávněné osoby dle čl. 13 této Smlouvy na jiném termínu, v elektronické podobě a s připomínkami jej předá zpět Zhotoviteli.
- 4.2 Zhotovitel zpracovává připomínky Objednatel ve lhůtě 5 pracovních dnů, nedohodnou-li se oprávněné osoby dle čl. 13 této Smlouvy na jiném termínu, a předá upravený dílčí celek Díla Objednateli, opět ve formátu MS Word (verze MS Word 2010 a vyšší). Objednatel ve lhůtě dohodnuté oprávněnými osobami potvrdí, že dílčí celek Díla nemá žádné vady ani nedodělky, nebo ve stejné lhůtě zpracovává formou revizí své připomínky.
- 4.3 V případě, že Objednatel potvrdí, že dílčí celek Díla dle čl. 1.1 bod (a) této Smlouvy nemá žádné vady ani nedodělky, zpracovává Zhotovitel tento dílčí celek Díla ve formátu *.pdf a MS Word (verze MS Word 2010 a vyšší) na CD v počtu 2 kusů a v písemné podobě v počtu 2 kusů a předá jej Objednateli, Smluvní strany

poté sepiší protokol o předání a převzetí dílčího plnění Díla, jehož vzor je uveden v **Příloze č. 2** tvořící nedílnou součást této Smlouvy. V případě, že Objednatel vyjádří k upravenému dílčímu celku Díla opět své připomínky, budou Smluvní strany postupovat v souladu s čl. 4.2 této Smlouvy.

- 4.4 Podmínkou pro zahájení plnění dílčího celku dle odst. 1.1 bodu (b) této Smlouvy je schválení Detailního návrhu řešení dle odst. 1.1 bod (a) této Smlouvy ze strany Objednatel. Zhotovitel je povinen dílčí plnění Díla dle odst. 1.1 bodu (b) této Smlouvy zhotovit podle schváleného Detailního návrhu řešení.
- 4.5 Veškeré dílčí celky Díla dle čl. 1.1 bod (a) a (b) budou předány Objednateli nejpozději v termínech dle harmonogramu plnění, který tvoří **Přílohu č. 4** této Smlouvy a na základě této **Přílohy č. 4** zpracovaného Detailního návrhu řešení dle odst. 1.1 bod (a) této Smlouvy. Zde uvedená termíny jsou konečné a nebudou dále měněny. To neplatí v případě změn Díla dle čl. 6 této Smlouvy.
- 4.6 Po dodání dílčích celků Díla dle čl. 1.1 bod (a) a (b) této Smlouvy předá Zhotovitel Objednateli za účelem testování Díla příslušné uživatelské a administrátorské dokumentace. O předání a převzetí bude sepsán předávací protokol, který podepíší oprávněné osoby Objednatel a Zhotovitel.
- 4.7 Po předání dle čl. 4.6 této Smlouvy této Smlouvy proběhne akceptační test za účasti Objednatel a Zhotovitel. Podrobný scénář akceptačního testu bude součástí Detailního návrhu řešení zpracovaného dle bodu 1.1 bodu (a) této Smlouvy. O průběhu a výsledcích akceptačních testů bude sepsán protokol, který bude obsahovat seznam zjištěných chyb a nedostatků a vyjádření, zda je Dílo způsobilé k akceptaci. Protokol podepíší odpovědní zástupci Objednatel a Zhotovitel.
- 4.8 Vyskytnou-li se během akceptačního testu jakékoliv vady, je Zhotovitel povinen tyto vady odstranit ve lhůtě dohodnuté oprávněnými osobami. Objednatel není povinen akceptovat dílčí celek Díla, ani podepsat Akceptační protokol, dokud tyto vady nebudou odstraněny. Jestliže vada dílčího celku Díla je nepodstatná, tzn., nemá vliv na řádnou funkčnost Díla, je Objednatel oprávněn akceptovat Dílo s výhradou s uvedením dosud trvajících nedostatků. Akceptace s výhradou nezabývá Zhotovitel povinnosti odstranit zbývající nedostatky / vady Díla. Podstatné vady Díla, které vždy brání a/nebo podstatně limitují Objednatel v řádném užívání Díla ve smyslu **Přílohy č. 1** tvořící nedílnou součást této Smlouvy.
- 4.9 Po podpisu Protokolu o výsledcích akceptačního testu s výsledkem, že předmět dílčího celku Díla je způsobilý k akceptaci dle čl. 4.8 této Smlouvy, podepíší oprávněné osoby Akceptační protokol, jehož vzor je uveden v **Příloze č. 3** tvořící nedílnou součást této Smlouvy. Pokud Objednatel do 10 pracovních dnů ode dne předložení Akceptačního protokolu Zhotovitelem k podpisu testu Akceptační protokol nepotvrdí ani k němu nesdělí žádné připomínky, považuje se takový Akceptační protokol za schválený.
- 4.10 Zhotovitel bude povinen na výzvu Objednatel zaškolit Objednatel určené administrátory a uživatele, a to v rozsahu dle čl. 3 přílohy č. 1 zadávací dokumentace Veřejné zakázky. Zaškolení příslušných osob Objednatel písemně

- potvrdí.
- 4.11 Den podpisu posledního protokolu či potvrzení ve vztahu k předmětu Díla bude považován za den řádného dokončení dílčí části Díla dle čl. 1.1 bod (b) této Smlouvy.
- 4.12 V rámci plnění části Díla dle čl. 1.1 bod (c) této Smlouvy bude Objednatel objednávat jednotlivé činnosti dle následujícího postupu:
- 4.12.1. Objednatel je oprávněn kdykoli v průběhu účinnosti této Smlouvy formou pokynu písemně zadat Zhotoviteli plnění (dále jen „Pokyn“) a Zhotovitel je povinen dle Pokynu nabídnout plnění, přičemž tento Pokyn musí obsahovat:
- a) konkrétní označení a bližší specifikaci plnění, které je zadáno;
 - b) termín dokončení plnění;
 - c) Objednatel předpokládá rozsah plnění, případně cenu za plnění stanovenou v souladu s cenovými podmínkami uvedenými v této Smlouvě.
- 4.12.2. V reakci na přijatý Pokyn Objednatel je Zhotovitel povinen do pěti (5) pracovních dnů doručit písemnou akceptaci Pokynu, nebo sdělit Objednateli vady Pokynu bránící Zhotoviteli poskytnout požadované plnění. Vadou dle tohoto odst. 5.4 této Smlouvy je zejména neurčitost zadání; vadou Pokynu také je, pokud obsahuje nepřiměřeně krátký termín plnění nebo nízký rozsah odhadované pracnosti, přičemž v takovém případě je Zhotovitel povinen tyto skutečnosti konkrétně a detailně specifikovat a odůvodnit. Objednatel je povinen odstranit případné vady Pokynu, které budou řádně specifikované Zhotovitelem a Pokyn opětovně předložit Zhotoviteli. Neodstraní-li Objednatel vady v Pokynu, je Zhotovitel povinen průběžně na trvání tohoto stavu Objednatel upozorňovat, a to až do té doby, než Objednatel rozhodne, že svoje Pokyn bere zpět, nebo specifikované vady odstraní.
- 4.13 Zhotovitel se zavazuje realizovat jakýkoliv Pokyn nebo požadavek vznesený Objednatel v souladu s touto Smlouvou.
- 4.14 Akceptace plnění dle čl. 1.1 bod (c) této Smlouvy, probíhá písemným schválením měsíčního výkazu poskytnutého plnění, jehož vzor je uveden v Příloze č. 8 této Smlouvy (dále jen „Výkaz plnění“), Objednatel.
- 4.15 Výkaz plnění předloží Zhotovitel Objednateli ke schválení nejpozději do pěti (5) dnů od skončení příslušného kalendářního měsíce. Objednatel ve lhůtě deseti (10) dnů ode dne předložení Výkazu plnění ke schválení tento Výkaz plnění schválí, nebo sdělí Zhotoviteli odůvodněné výhrady k obsahu předloženého Výkazu plnění, zejména tehdy, pokud Výkaz plnění neodpovídá skutečně poskytnutému plnění v daném měsíci. Zhotovitel na základě výhrad Objednatel předloží opravený Výkaz plnění do pěti (5) dnů ode dne obdržení výhrad Objednatel. Schválení opraveného Výkazu plnění se řídí tímto ustanovením. Tento postup lze použít i opakovaně.
- 4.16 Místem předání a převzetí Díla včetně jeho jednotlivých dílčích celků je sídlo

Objednatel uvedeně v této Smlouvě, pokud se Smluvní strany nedohodnou jinak.

5 PLATEBNÍ PODMÍNKY

- 5.1 Objednatel uhradí Zhotoviteli Cenu za Dílo po částech, a to následovně:
- a) část Ceny odpovídající ceně za dílčí Dodávku předmětu Smlouvy, dle **Přílohy č. 5 písm. A) Fáze 1**, této Smlouvy na základě daňového dokladu, který Zhotovitel vystaví po oboustranném podpisu protokolu o předání a převzetí dílčí části Díla dle čl. 4.3 této Smlouvy,
 - b) část Ceny odpovídající ceně za dílčí Dodávku předmětu Smlouvy, dle **Přílohy č. 5 písm. A) Fáze 2**, této Smlouvy na základě daňového dokladu, který Zhotovitel vystaví po oboustranném podpisu protokolu o předání a převzetí dílčí části Díla dle čl. 4.3 této Smlouvy,
 - c) část Ceny odpovídající ceně za Dodávku služeb podpory výrobce, školení a služeb podpory provozu a zpracování dokumentace dle čl. 4.6 této Smlouvy dle **Přílohy č. 5 písm. B)** na základě daňového dokladu, který Zhotovitel vystaví po oboustranném podpisu protokolu o předání a převzetí dílčí části Díla dle čl. 4.11 této Smlouvy,
 - d) část Ceny odpovídající ceně za poskytnuté plnění dle čl. 1.1 bod (c) této Smlouvy na základě daňového dokladu, který Zhotovitel vystaví po schválení Výkazu plnění dle čl. 4.15 této Smlouvy.
- 5.2 Zhotovitel není oprávněn požadovat jakékoli zálohy.
- 5.3 Zhotovitel není oprávněn požadovat jakékoli zálohy. Faktury musí mít veškeré náležitosti daňového dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a jejich přílohou budou příslušná potvrzení Objednatel podle ustanovení čl. 4 této Smlouvy podepsaná oprávněnými osobami uvedenými v čl. 13 této Smlouvy. Faktury budou dále obsahovat zejména následující údaje:
- (i) číslo Smlouvy, označení případných dodatků Smlouvy;
 - (ii) číslo a název příslušné veřejné zakázky;
 - (iii) popis plnění Zhotovitele.
- 5.4 Daňový doklad (faktura) vystavený Zhotovitelem podle této Smlouvy bude Zhotovitel vždy ve dvou vyhotovených zaslát Objednateli a jeho splatnost bude činit 30 kalendářních dnů ode dne doručení Objednateli. Za den úhrady daně faktury bude považován den odesání fakturované částky z účtu Objednatel.
- 5.5 Objednatel si vyhrazuje právo vrátit Zhotoviteli do data jeho splatnosti daňový doklad (fakturu), který nebude obsahovat veškeré údaje vyžadované závaznými právními předpisy ČR nebo touto Smlouvou, nebo v něm budou uvedeny nesprávné údaje (s uvedením chybějících náležitostí nebo nesprávných údajů) anebo nebude doložen některým v čl. 4 této Smlouvy uvedených potvrzení Objednatel podepsaným oprávněnými osobami uvedenými v čl. 13 této

Smlouvy. V takovém případě začne běžet doba splatnosti daňového dokladu (faktury) až doručení řádně opraveného daňového dokladu (faktury) Objednateli.

6 ZMĚNY DÍLA V PRŮBĚHU PLNĚNÍ

- 6.1 Objednatel je podle této Smlouvy oprávněn kdykoliv požadovat po Zhotoviteli změny Díla nebo jeho dílčích plnění. Zhotovitel je povinen provést veškeré změny požadované Objednatelům pouze za předpokladu splnění podmínky stanovené v čl. 6.3 této Smlouvy.
- 6.2 Zhotovitel je podle této Smlouvy oprávněn kdykoliv navrhnout Objednateli změny Díla nebo jeho dílčích plnění, přispějí-li k větší funkčnosti a zlepšení vlastností Díla nebo jeho dílčích plnění. Objednatel však není povinen návrh jakékoliv změny předložený Zhotovitelem přijmout.
- 6.3 Veškeré změny Díla nebo jeho dílčích plnění podle čl. 6.1 a 6.2 této Smlouvy musí být odsouhlaseny oběma Smluvními stranami a sjednány písemně dodatkem k této Smlouvě a musí být v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Zhotovitel není povinen provést jakékoliv změny Díla a Objednatel není povinen převzít jakékoliv změny Díla, dokud nebudou písemně odsouhlaseny a sjednány dodatkem k této Smlouvě.

7 PRÁVA A POVINNOSTI ZHOTOVITĚLE

- 7.1 Zhotovitel je povinen provést Dílo řádně a včas v souladu s harmonogramem plnění uvedeným v **Příloze č. 4** této Smlouvy a v Detailním návrhu řešení.
- 7.2 Zhotovitel je povinen postupovat při provádění Díla s náležitou odbornou péčí a podle pokynů Objednatel. Při provádění Díla je Zhotovitel povinen upozorňovat Objednatel na nevhodnost jeho pokynů, které by mohly mít za následek újmu na právech Objednatel nebo vznik škody. Pokud Objednatel i přes upozornění na splnění svých pokynů trvá, neodpovídá Zhotovitel za případnou škodu tím vzniklou.
- 7.3 Smluvní strany sjednaly, že Zhotovitel je oprávněn k plnění této Smlouvy použít třetích osob (pododávatele) i bez předchozího souhlasu Objednatel a to zejména třetích osob, uvedených v nabídce Zhotovitel a na předmětnou veřejnou zakázku.
- 7.4 Zhotovitel se zavazuje využít při plnění této Smlouvy v daných rolích pouze osoby uvedené v **Příloze č. 7** této Smlouvy.
- 7.5 Jakákoliv dodatečná změna členů týmu uvedených v **Příloze č. 7** této Smlouvy musí být předem písemně schválena Objednatel. Poskytovatel se v takovém případě zavazuje nahradit osobu člena týmu takovou osobou, která disponuje alespoň obdobnými znalostmi, zkušenostmi a odbornou kvalifikací jako u nahrazovaného člena týmu.

7.6 Jednotliví členové realizačního týmu musí být držiteli osvědčení a certifikace, jak je uvedena v **Příloze č. 7** této Smlouvy. Poskytovatel se zavazuje, že po celou dobu trvání této Smlouvy bude u jednotlivých členů realizačního týmu udržovat certifikaci minimálně v uvedeném rozsahu a úrovni.

7.7 Objednatel je kdykoliv po dobu trvání této Smlouvy oprávněn po Poskytovateli požadovat prokázání splnění požadavků na členy realizačního týmu dle čl. 7.6 této Smlouvy, resp. dle požadavků uvedených v **Příloze č. 7** této Smlouvy, a to u kteréhokoliv člena realizačního týmu, a Poskytovatel je povinen bezodkladně, nejpozději však do 5 pracovních dnů po vznesení takového požadavku Objednatel, toto Objednateli náležitě prokázat.

7.8 Všechna data, ať už v jakékoliv podobě, a jejich hmotné nosiče, která vznikla či vzniknou při provádění Díla podle této Smlouvy, jsou výlučným vlastnictvím Objednatel. Nejpozději do 15 pracovních dnů od doručení žádosti Objednatel nebo od ukončení této Smlouvy je Zhotovitel povinen tato data a jejich nosiče Objednateli předat.

7.9 Zhotovitel není oprávněn použít podklady, data a hmotné nosiče předané mu pro realizaci Díla Objednatel pro jiné účely než je provedení Díla podle této Smlouvy. Nejpozději do 15 pracovních dnů po ukončení této Smlouvy je Zhotovitel povinen vrátit Objednateli veškeré podklady, data a hmotné nosiče poskytnuté Objednatel Zhotoviteli ke splnění jeho povinnosti podle této Smlouvy.

7.10 Zhotovitel není oprávněn bez předchozího písemného souhlasu Objednatel (i) provádět jakékoli zápočty svých pohledávek vůči Objednateli proti jakýmkoli pohledávkám Objednatel za Zhotovitelem, ani (ii) postupovat jakoukoli svoje práva a pohledávky vůči Objednateli na jakoukoli třetí osobu.

7.11 Zhotovitel není oprávněn zpřístupnit Dílo či jakékoli jeho dílčí celky jakýmkoli třetí osobám vyjma pododávatelů ve smyslu čl. 7.3 této Smlouvy.

7.12 V případě, že se vyskytně jakákoliv překážka, zejména

(i) prodlení Objednatel s poskytnutím součinnosti, které by podmiňovalo plnění Zhotovitel;

(ii) mimořádná nepředvídatelná a neprognostická překážka vzniklá nezávisle na vůli Zhotovitel, jak je vymezena v ustanovení § 2913 odst. 2 obč. zák. apod.,

která by mohla mít jakýkoliv dopad do termínů plnění Díla, má Zhotovitel povinnost o této překážce Objednatel písemně informovat, a to nejpozději do pěti (5) kalendářních dnů od okamžiku, kdy se o této překážce dozvěděl. Pokud Zhotovitel Objednatel v této písemné informaci o překážkách písemně neinformuje, zanikají veškerá práva Zhotovitel, která se na existenci příslušné překážky vztá, zejména Zhotovitel nebude mít nárok na jakékoli posunutí termínů plnění Díla.

7.13 Zhotovitel je povinen uzavřít a po celou dobu trvání této Smlouvy a dále nejméně po dobu záruční doby podle čl. 9.1 této Smlouvy udržovat pojistnou smlouvu na

škodu způsobenou třetími osobami s limitem pojistného plnění alespoň na částku ve výši 30.000.000,- Kč.

7.14 V případě, že po řádné fungování Díla v rozsahu stanoveném touto Smlouvou a přiblížení této Smlouvy je nutná součinnost třetích osob, je Zhotovitel povinen takovou součinnost pro Objednatel smluvně zajistit.

8 PRÁVA A POVINNOSTI OBJEDNATELE

8.1 Objednatel je povinen poskytnout Zhotoviteli ke splnění Díla součinnost podle Detailního návrhu řešení, případně zajistit její poskytnutí třetími osobami.

8.2 Pokud Objednatel neposkytne v čl. 8.1 této Smlouvy dohodnutou součinnost, má Zhotovitel právo požadovat na Objednateli posunutí stanovených termínů o čas, po který Zhotovitel nemohl pracovat na plnění předmětu Smlouvy v důsledku neposkytnutí součinnosti ze strany Objednatel.

8.3 Objednatel je povinen Zhotoviteli poskytnout veškeré podklady a informace nezbytné k provedení Díla.

9 ODPOVĚDNOST ZA VADY

9.1 Zhotovitel odpovídá za to, že Dílo bude provedeno řádně, v souladu s touto Smlouvou a bude prosté jakýchkoli vad (za věcnou vadu bude zejména považován rozpor mezi skutečnou funkcí Díla a jeho funkcí popsanou v této Smlouvě) po dobu účinnosti Smlouvy o zajištění provozu a podpory, v žádném případě však po dobu kratší než 36 měsíců.

9.2 Záruční doba na předmět díla dle čl. 9.1 této Smlouvy počíná běžet dnem podpisu protokolu dle čl. 4.9 této smlouvy oprávněnými osobami uvedenými v čl. 13 této Smlouvy.

9.3 Zhotovitel dále zaručuje, že Dílo nebude zatíženo žádnými nároky, požadavky, zástavním právem, břemeny nebo jinými právy třetích osob, které by překážely klidnému užívání Díla Objednatel, a že bude prosté všech právních vad.

9.4 Zhotovitel zaručuje, že po dobu trvání záruční doby dle čl. 9.1 této Smlouvy bude bez vad fungovat propojení Díla se stávajícími informačními systémy Objednatel uvedenými v **Příloze č. 6** této Smlouvy.

9.5 Po záruční dobu bude Zhotovitel povinen odstranit veškeré vytčené vady Díla ve lhůtách a za podmínek uvedených v této smlouvě.

10 SANKCE

10.1 V případě prodlení Objednatel s platbou Ceny za Dílo bude Objednatel povinen uhradit Zhotoviteli úrok z prodlení ve výši 0,05 % z dlužné částky za každý započatý den prodlení.

10.2 V případě, že Zhotovitel poruší svou povinnost předat Objednateli dílčí část Díla řádně a včas v souladu s čl. 2.2 této Smlouvy, bude povinen zaplatit Objednateli smluvní pokutu 0,05 % z částí Ceny dle příslušného platebního milníku dle **Přílohy č. 5** této Smlouvy, a to za každý započatý den prodlení s předáním příslušné dílčí části Díla.

10.3 V případě, že Zhotovitel poruší svou povinnost odstranit vady Díla vytčené Objednatel v souladu s čl. 4.9 a/nebo čl. 9.5 této Smlouvy, bude povinen zaplatit Objednateli smluvní pokutu ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každý započatý den prodlení s odstraněním vad Díla. Po dobu účinnosti Smlouvy o zajištění provozu a podpory však budou uplatňovány smluvní pokuty tam uvedené.

10.4 V případě porušení povinnosti poskytovat plnění dle této Smlouvy prostřednictvím osob s potřebnou certifikací dle čl. 7.6 této Smlouvy má Objednatel nárok na smluvní pokutu ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každý i započatý den poskytování Služby osobou bez potřebné certifikace.

10.5 V případě porušení povinnosti předložit podklady prokazující splnění požadavků na členy realizačního týmu ve lhůze dle čl. 7.7 této Smlouvy má Objednatel nárok na smluvní pokutu ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každý i započatý den prodlení s předložením potvrzení.

10.6 V případě, že Zhotovitel poruší svou povinnost zachovávat mlčenlivost, nezpřístupnit třetí osobám nevěřejné informace a/nebo podniknout veškeré nezbytné kroky k zabezpečení těchto informací dle čl. 11.2 a 11.6 této Smlouvy a/nebo Zhotovitel v rozporu s čl. 11.7 této Smlouvy použije nevěřejné informace jinak než za účelem plnění této Smlouvy a/nebo Zhotovitel poruší svou povinnost zavázat svého případného pododávatele povinností mlčenlivosti a respektováním práv Objednatel dle ustanovení čl. 11.8 této Smlouvy a/nebo Zhotovitel poruší své povinnosti vztahující se k ochraně osobních údajů dle čl. 11.11 této Smlouvy, bude povinen zaplatit Objednateli smluvní pokutu ve výši 200.000,- Kč (slovy: dvě stě tisíc korun českých) za každé takové porušení.

10.7 V případě, že Zhotovitel v rozporu s čl. 7.9 této Smlouvy použije podklady, data a hmotné nosiče předané mu Objednatel dle této Smlouvy pro jiné účely než je poskytování Služby podle této Smlouvy a/nebo ve stanoveném termínu nevrátí Objednateli veškeré podklady, data a hmotné nosiče poskytnuté Objednatel Zhotoviteli ke splnění jeho závazků podle této Smlouvy, bude Zhotovitel povinen zaplatit Objednateli smluvní pokutu ve výši 1.000,- Kč (slovy: jeden tisíc korun českých) za každý den trvání takového porušení.

10.8 V případě, že Zhotovitel poruší povinnost uzavřít nebo po celou dobu trvání této Smlouvy udržovat pojistnou smlouvu na škodu způsobenou třetími osobami s limitem pojistného plnění alespoň na částku 30.000.000,- Kč (slovy: třicet milionů korun českých), bude povinen zaplatit Objednateli smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý započatý den trvání porušení této povinnosti.

10.9 Smluvní pokuty stanovené dle tohoto čl. 10 jsou splatné do 30 dnů ode dne doručení výzvy oprávněné strany k zaplacení smluvní pokuty povinné Smluvní straně.

10.10 Objednatel je oprávněn kdykoliv provést zápočet svých pohledávek vůči Zhotoviteli vzniklých v souladu s tímto článkem 10 proti jakýmkoli splatným pohledávkám Zhotovitel za Objednatel, zejména pohledávkám na zaplacení Ceny.

10.11 Smluvní strany odchýlně od ustanovení § 2050 Občanského zákoníku sjednaly, že zaplacením jakékoliv smluvní pokuty podle této Smlouvy není dotčena povinnost Zhotovitele nahradit Objednateli v plné výši též škodu vzniklou porušením povinností, na kterou se smluvní pokuta vztahuje.

11 OCHRANA DŮVĚRNÝCH INFORMACÍ

11.1 Ochranu utajovaných informací zajistí obě Smluvní strany v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a předpisů souvisejících.

11.2 Obě Smluvní strany jsou povinny zachovávat mlčenlivost a nezpřístupnit třetím osobám neveřejné informace (jak jsou vymezeny níže). Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.

11.3 Za neveřejné informace se považují veškeré následující informace:

- veškeré informace poskytnuté Objednatelům Zhotoviteli v souvislosti s touto Smlouvou;
- informace, na které se vztahuje zákonem uložená povinnost mlčenlivosti Objednatelů;
- veškeré další informace, které budou Objednatelům či Zhotoviteli označeny jako neveřejné ve smyslu ustanovení § 218 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

11.4 Povinnost zachovávat mlčenlivost uvedená v tomto čl. 11 se nevztahuje na informace:

- kteří jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením právních povinností ze strany Zhotovitele,
- jejichž sdělení se vyžaduje ze zákona.

11.5 Neveřejné informace zahrnují rovněž veškeré informace získané náhodně nebo bez vědomí Zhotovitele a dále veškeré informace získané od jakýchkoli třetí strany, které se týkají Objednatelů či plnění této Smlouvy.

11.6 Smluvní strany jsou povinny nezpřístupnit jakékoliv třetí osobě, výjima poddávatele Zhotovitele ve smyslu čl. 7.3 této Smlouvy, neveřejné informace druhé Smluvní strany bez jejího souhlasu, a to v jakékoliv formě, a podniknout všechny nezbytné kroky k

zabezpečení těchto informací. Zhotovitel je povinen zabezpečit veškeré neveřejné informace Objednatelů proti odcizení nebo jinému zneužití.

11.7 Zhotovitel je povinen neveřejné informace užívat pouze a účelem plnění této Smlouvy. Jiná použití nejsou bez písemného svolení Objednatelů přípustná.

11.8 Zhotovitel je povinen svého případného poddávatele zavázat povinností mlčenlivosti a respektováním práv Objednatelů nejméně ve stejném rozsahu, v jakém je v tomto závazkovém vztahu zavázán sám.

11.9 Povinnost mlčenlivosti podle tohoto čl. 11 Smlouvy trvá po dobu 5 let od ukončení této Smlouvy.

11.10 Za prokázané porušení povinností dle tohoto čl. 11 Smlouvy má druhá Smluvní strana právo požadovat náhradu takto vzniklé škody.

11.11 Za neveřejné informace se považují vždy veškeré osobní údaje podle zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Shromažďovat a zpracovávat osobní údaje zaměstnanců a jiných osob, eventuelně citlivé osobní údaje lze jen v případech stanovených zákonem, nebo se souhlasem nositele osobních údajů. Zhotovitel není oprávněn zpřístupňovat osobní údaje zaměstnanců a jiných osob, se kterými bude v průběhu plnění této smlouvy seznámen, třetím osobám a rovněž není oprávněn je jakýmkoliv způsobem zveřejnit.

11.12 Nelehde na ustanovení článků 11.1 až 11.7 této Smlouvy Zhotovitel dále výslovně souhlasí s tím, aby tato Smlouva byla v plném rozsahu uveřejněna na webových stránkách určených Objednatelům. Smluvní strany prohlašují, že skutečnosti uvedené v této Smlouvě nepovažují za obchodní tajemství ve smyslu § 504 Občanského zákoníku a udělují svolení k jejich užití a uveřejnění bez stanovení jakýchkoli dalších podmínek.

12 UKONČENÍ SMLOUVY

12.1 Tato Smlouva může být před řádným dokončením Díla ukončena pouze na základě dohody obou Smluvních stran nebo odstoupením Smluvní strany v souladu s tímto článkem.

12.2 Objednatel je oprávněn odstoupit od této Smlouvy v případě, že Zhotovitel je v prodlení s prováděním Díla nebo kteréhokoliv dílčího plnění po dobu delší než 30 dnů oproti termínům sjednaným v časovém harmonogramu, který tvoří **Přílohu č. 4** této Smlouvy a/nebo Detailní návrh řešení a nezjedná nápravu ani do 5 pracovních dnů od doručení písemné výzvy Objednatelů.

12.3 Zjistí-li Objednatel, že Zhotovitel porušuje některou ze svých smluvních povinností či zákonných povinností, které se vztahují k provádění Díla, může požadovat, aby Zhotovitel zajistil nápravu a prováděl Dílo řádným způsobem. Neutínil-li tak Zhotovitel ani v přiměřené době, Objednatel může obdobně dle ustanovení § 2593 obč. zák. odstoupit od této Smlouvy, vedl-li by postup Zhotovitele k jejímu podstatnému porušení.

12.4 Zhotovitel je oprávněn odstoupit od této Smlouvy v případě, že nedojde k podpisu Akceptačního protokolu dílčího celku dle čl. 1.1 bod (b) této Smlouvy v souladu s čl. 4 této Smlouvy ze strany Objednatelů ani k sdělení připomínek po dobu delší než 30 dnů ode dne předání tohoto dílčího celku Zhotovitelem k připomínkám dle čl. 4 této Smlouvy.

12.5 Objednatel je dále oprávněn odstoupit od této Smlouvy v případě, že se prokáže, že Dílo nebo jeho část (či data) je zatížena právy třetí osoby, a Zhotovitel nezíská tyto chybné práva nebo nenahradí zatížené dílčí části Díla nezatíženými ani do 15 pracovních dnů od doručení písemné výzvy Objednatelů.

12.6 Objednatel je rovněž oprávněn odstoupit od této Smlouvy v případě, že z důvodů na straně Zhotovitele nedojde k podpisu protokolu o předání a převzetí Detailního návrhu řešení dle čl. 4.3 této Smlouvy nejpozději do 2 měsíců ode dne jeho předložení Objednatelům dle čl. 4.1 této Smlouvy.

12.7 Zhotovitel je oprávněn odstoupit od této Smlouvy v případě, že Objednatel je v prodlení s platbou Ceny za Dílo po dobu delší než 45 dnů po splatnosti příslušného daňového dokladu a nezjedná nápravu ani do 5 pracovních dnů od doručení písemné výzvy Zhotovitele k nápravě.

12.8 Odstoupení od Smlouvy je účinné okamžikem doručení písemného oznámení o odstoupení příslušné Smluvní straně. Smluvní strany sjednaly, že si nebudou vracet vzájemně poskytnutá plnění, přičemž od Smlouvy lze odstoupit pouze ohledně nesplněného zbytku plnění.

12.9 Ukončením této Smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, ochrany důvěrných informací, práva na náhradu škody vzniklé z porušení smluvní povinností a ustanovení týkající se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po skončení účinnosti této Smlouvy.

13 OPRÁVNĚNÉ OSOBY

13.1 Komunikace mezi Smluvními stranami bude probíhat zejména prostřednictvím následujících oprávněných osob, pověřených pracovníků nebo statutárních zástupců Smluvních stran:

(i) Oprávněnými osobami Objednatelů jsou:
ve věcech smluvních:

[redacted]
ve věcech technických a protokolů:
[redacted]

(ii) Oprávněnými osobami Zhotovitele jsou:

[redacted]

13.2 Oprávněné osoby, nejsou-li statutárním orgánem, nejsou oprávněny ke změnám této Smlouvy, jejím doplňkům ani zrušení, ledaže se prokáže plnou mocí udělenou jim k tomu osobami oprávněnými jednat navenek za příslušnou Smluvní stranu v záležitostech této Smlouvy. Smluvní strany jsou oprávněny

jednostranně změnit oprávněné osoby, jsou však povinny takovou změnu druhé Smluvní straně bezodkladně písemně oznámit.

13.3 Veškeré uplatňování nároků, sdělování, žádosti, předávání informací apod. mezi Smluvními stranami dle této Smlouvy musí být příslušnou Smluvní stranou provedeno v písemné formě a doručeno druhé Smluvní straně osobně, doporučenou poštou, nebo e-mailem s použitím elektronického podpisu, není-li v této Smlouvě sjednáno jinak.

14 PRÁVA K DÍLU

14.1 Objednatel nabývá právo užívat Díla, resp. dílčího plnění, a to včetně dat, která tvoří součást plnění podle této Smlouvy a nejsou předmětem práv na ochranu duševního vlastnictví:

- okamžikem podpisu Protokolu o předání a převzetí, resp. podpisem Akceptačního protokolu, není-li Protokol o předání a převzetí vyhotovován;
- okamžikem zabudování věcí do stávajících struktur Objednatelů, či provedením prací či služeb na stávajícím vybavení Objednatelů;
- okamžikem jejich zaplacení;

podle toho, která z výše uvedených skutečností nastane dříve.

14.2 Nebezpečí škody na Díle přejde na Objednatelů okamžikem podpisu Protokolu o předání a převzetí, resp. podpisem Akceptačního protokolu, není-li Protokol o předání a převzetí vyhotovován.

14.3 Vzhledem k tomu, že součástí plnění Zhotovitele dle této Smlouvy je i plnění, které může naplňovat znaky autorského díla ve smyslu 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“), je k těmto součástem plnění poskytována licence za podmínek sjednaných v tomto článku Smlouvy.

14.4 Objednatel je oprávněn veškeré součásti plnění a veškeré výstupy Zhotovitele považované za autorské dílo ve smyslu autorského zákona (dále jen „autorská díla“) užívat dle podmínek stanovených touto Smlouvou.

14.5 Zhotovitel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorským dílům, které budou součástí plnění podle této Smlouvy, resp. že má souhlas všech relevantních třetích osob k poskytnutí licence k autorským dílům podle tohoto článku Smlouvy; toto prohlášení zahrnuje i taková práva, která by vytvořením autorského díla teprve vznikla.

14.6 Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k autorskému dílu užívat toto autorské dílo v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené s ohledem na účel této Smlouvy. Pro vyloučení pochybností to znamená, že Objednatel je s ohledem na účel této Smlouvy oprávněn užívat autorské dílo v neomezeném množstevním rozsahu a územním rozsahu omezeném na území ČR, a to všemi v úvahu přicházejícími způsoby užití a s časovým rozsahem omezeným pouze dobou trvání majetkových autorských práv

k takovému autorskému dílu. Objednatel je bez potřeby jakéhokoliv dalšího svolení Zhotovitele oprávněn udělit třetí osobě podlicenci k užití autorského díla nebo svoje oprávnění k užití autorského díla třetí osobě postoupit, avšak pouze za předpokladu, že tím bude docházet k užití autorského díla v souladu s účelem, pro který byla licence k němu Objednateli poskytnuta. Licence k autorskému dílu je poskytována jako nevýhradní. Objednatel není povinen licenci využít.

- 14.7 V případě počítačových programů se licence vztahuje na autorské dílo ve strojovém kódu, jakož i související dokumentaci. Předchozí věta tohoto odstavce se vztahuje i na případně další verze software nebo jiných informačních systémů upravených na základě této Smlouvy.
- 14.8 Zhotovitel touto Smlouvou poskytuje Objednateli licenci k autorským dílům dle odst. 14.3 této Smlouvy, přičemž účinnost této licence nastává okamžikem akceptace součástí plnění, které příslušné autorské dílo obsahuje; do té doby je Objednatel oprávněn autorské dílo užívat v rozsahu a způsobem nezbytným k provedení akceptace příslušné součásti plnění.
- 14.9 Udělení licence nelze ze strany Zhotovitele vypovědět a její účinnost trvá i po skončení účinnosti této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak.
- 14.10 Smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle této Smlouvy vznikne činnost Zhotovitele a Objednatel dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Zhotovitel udělil Objednateli souhlas k jakémukoli změně nebo jinému zásahu do díla spoluautorů. Cena dle této Smlouvy je stanovena se zohledněním tohoto ustanovení a Zhotoviteli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.
- 14.11 Zhotovitel je povinen postupovat tak, aby udělení licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci zabezpečil, a to bez újmy na právech třetích osob.
- 14.12 Případná změna v osobě Zhotovitele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Zhotovitelem Objednateli.
- 14.13 Odměna za poskytnutí, zprostředkování nebo postoupení licence k autorskému dílu je zahrnuta v ceně za plnění, při němž došlo k vytvoření autorského díla.

15 ZÁVĚREČNÁ UJEDNÁNÍ

- 15.1 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy.
- 15.2 Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami. Tato Smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
- 15.3 Smluvní strany výslovně sjednávají, že uveřejnění této smlouvy v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých

smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) zajistí Objednatel.

- 15.4 Vyjma změn osob uvedených v čl. 7.5 této Smlouvy a oprávněných osob podle čl. 13 této Smlouvy mohou veškeré změny a doplňky této Smlouvy být provedeny pouze po dosažení úplného konsenzu na obsahu změny či doplňku, a to písemným dodatkem k této Smlouvě podepsaným osobami oprávněnými zastupovat obě Smluvní strany. Smluvní strany tedy vylučují možnost uzavření dodatku bez ujednání o veškerých náležitostech dle § 1726 obč. zák. Smluvní strany rovněž vylučují použití ustanovení § 1740 odst. 3 a ustanovení § 1757 odst. 2 obč. zák.
- 15.5 Zhotovitel tímto výslovně prohlašuje, že v souladu s ustanovením § 1765 odst. 2 obč. zák. na sebe bere nebezpečí změny okolností.
- 15.6 Tato Smlouva a všechny vztahy z ní vyplývající se řídí právním řádem České republiky. Obchodních podmínek kterékoliv Smluvní strany se použije, pouze pokud to tato Smlouva, resp. její změny nebo doplňky výslovně stanovují.
- 15.7 Spor, který vznikne na základě této Smlouvy nebo který s ní souvisí, jsou Smluvní strany povinny řešit přednostně smírnou cestou, pokud možno do 30 dnů ode dne, kdy o sporu jedna Smluvní strana uvědomí druhou Smluvní stranu. Jinak jsou pro řešení sporů z této Smlouvy příslušné obecné soudy České republiky.
- 15.8 V případě, že některé ustanovení této Smlouvy je nebo se stane v budoucnu neplatným, neúčinným či nevymahatelným nebo bude-li takovým příslušným orgánem shledáno, zůstávají ostatní ustanovení této Smlouvy v platnosti a účinnosti pokud z povahy takového ustanovení nebo z jeho obsahu anebo z okolností, za nichž bylo uzavřeno, nevyplyvá, že je nelze oddělit od ostatního obsahu této Smlouvy. Smluvní strany jsou povinny nahradit neplatné, neúčinné nebo nevymahatelné ustanovení této Smlouvy ustanovením jiným, které svým obsahem a smyslem odpovídá nejlépe ustanovení původnímu a této Smlouvě jako celku.
- 15.9 Tato Smlouva je vyhotovena ve čtyřech (4) vyhotoveních v českém jazyce, přičemž všechna vyhotovení mají platnost originálu. Tři (3) vyhotovení Smlouvy obdrží Objednatel a jedno (1) Zhotovitel.
- 15.10 Nedílnou součástí této Smlouvy jsou následující přílohy:

- Příloha č. 1:** Specifikace předmětu plnění
Příloha č. 2: Vzor Protokolu o předání a převzetí
Příloha č. 3: Vzor Akceptačního protokolu
Příloha č. 4: Harmonogram plnění
Příloha č. 5: Podrobná specifikace ceny
Příloha č. 6: Náhrádka Zhotovitele
Příloha č. 7: Seznam členů realizačního týmu
Příloha č. 8: Vzor Výkazu plnění a protokol o převzetí plnění

- 15.11 V případě rozporu mezi textem této Smlouvy a textem přílohy má přednost ustanovení textu této Smlouvy. V případě jakéhokoliv nejistoty ohledně výkladu budou ustanovení této Smlouvy vykládána tak, aby v co nejširší míře zohledňovala účel veřejné zakázky vyjádřený ve výzvě k podání nabídky a zadávací dokumentaci veřejné zakázky. V případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení výzvy k podání nabídek a zadávací dokumentace veřejné zakázky. Zhotovitel je vázán svou nabídkou na Veřejnou zakázku předloženou Objednateli, která tvoří **Přílohu č. 6** této Smlouvy a pro úpravu vzájemných vztahů vyplývajících z této Smlouvy se použije subsidiárně.

- 15.12 Smluvní strany výslovně souhlasí, aby byla tato Smlouva uveřejněna v Centrální evidenci smluv (CES), vedené Objednatel, která je veřejně přístupná. Dále Zhotovitel prohlašuje, že skutečnosti uvedené v této Smlouvě nepovažuje za obchodní tajemství ve smyslu ustanovení § 504 občanského zákoníku a uděluje svolení s jejich uveřejněním.
- 15.13 Tato Smlouva byla schválena Radou hlavního města Prahy usnesením č. [redacted] ze dne [redacted] nadpoloviční většinou hlasů členů Rady hlavního města Prahy.
- 15.14 Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

V Praze dne _____

V Praze dne 27. 06. 2018

Objednatel:

Zhotovitel:

Hlavní město Praha

Corpus Solutions a.s.

Podpis:

Podpis:

Jméno:

Jméno:

Funkce: ředitel odboru INF HMP

Funkce: člen představenstva

Digitálně podepsal
Ivo Musil
Datum: 2018.07.02
09:11:05 +02'00'

PŘÍLOHA č. 1

TECHNICKÁ SPECIFIKACE

Tato příloha je nedílnou součástí zadávací dokumentace veřejné zakázky s názvem

„Bezpečné síťové prostředí“

Obsahuje podrobné vymezení předmětu veřejné zakázky. Požadavky specifikované v příložených tabulkách této přílohy považuje Zadavatel za minimální a na jejich splnění Zadavatel trvá.

Předmět veřejné zakázky se skládá z následujících částí:

1. Vypracování Detailního návrhu řešení,
2. Dodávka technologií Bezpečného síťového prostředí,
3. Instalace a implementace Bezpečného síťového prostředí,
4. Služby úpravy konfigurace současných bezpečnostní technologií,
5. Poskytnutí služeb podpory výrobců technologie, dle skupin produktů, na 3 a 4 roky od ukončení instalace a implementace,
6. Poskytnutí školení a servisní podpory spojené s provozem technologie
7. Poskytování dalších odborných služeb

Dílo bude realizováno a předáváno po etapách. Etapy vycházejí z hrubého harmonogramu, které jsou uvedeny v čl. 7 této přílohy ZD. Začátek každé etapy je vázán na protokolární převzetí předchozí etapy Zadavatelem na základě akceptačního protokolu.

Obsah

1. Vypracování Detailního návrhu řešení	26
2. Dodávka technologií Bezpečného síťového prostředí	29
3. Instalace a implementace Bezpečného síťového prostředí	114
4. Úpravy konfigurací současných bezpečnostních technologií	116
5. Poskytnutí služeb podpory výrobců technologie	118
6. Poskytnutí školení a servisní podpory spojené s provozem technologie	119
7. Poskytování dalších odborných služeb	120
8. Harmonogram	121
9. Ostatní požadavky	122
10. Součinnost zadavatele	122

1. Vypracování Detailního návrhu řešení

Dodavatel samostatně vypracuje do 6 týdnů od podpisu smlouvy Detailní návrh řešení.

Detailní návrh řešení bude obsahovat minimálně Elenění na tyto kapitoly:

- o Místní šetření - detailní analýza ve všech dotčených lokalitách
- o Zpracování High-Level a Low-level designu síťové topologie
- o Vytvoření prováděcího projektu, projektové přípravy a návrh dohodnutí součinnosti
- o Předložení Detailního návrhu řešení Zadavateli

Detailní návrh řešení bude vypracován ve dvou etapách 1 a 2.

Etapa č. 1 - Místní šetření

1. Analýza - místní šetření - ve všech dotčených lokalitách s cílem zjistit všechny detailní informace potřebné pro vypracování prováděcího projektu.
2. Specifikace hardware, který bude součástí dodávky řešení
3. Vytvoření prováděcího projektu, Projektová příprava, dohodnutí součinnosti, apod.
4. Bodou provedeny workshopy s garanti navazujících částí infrastruktury MHMP (servery, bezpečnost, aplikace, ...) s cílem definovat vzájemné vazby a identifikovat rizika migrace. Zjistitelné informace budou zaneseny do prováděcího projektu v rámci etapy č. 2.
5. Zkreslení tzv. High-Design and Low-Design sítě
6. Specifikace požadavků na provozní prostředí, např. mohou být identifikovány potřeby nutné pro realizaci migrace (zajištění napájení, místa v rackech apod.)

Etapa č. 2 - Prováděcí projekt

V rámci této části bude upřesněn detail ohledně umístění a nastavení jednotlivých zařízení. Bude se jednat primárně o definici a popsání následujících údajů:

7. přesné rozmístění jednotlivých zařízení
8. stanovení způsobu propojení zařízení až na úrovni konkrétních portů, IP adres, konektorů apod.
9. vytvoření migračního plánu pro každý funkční blok síťové infrastruktury
10. definování garantů v jednotlivých lokalitách a stanovení klíčových uživatelů pro ověřování funkčnosti systémů
11. pojmenování dopadů do stávající infrastruktury (rekonfigurace serverů, aplikací, operátorských linek, Mepnetu apod.) a zajištění součinnosti jejich správců
12. bude vytvořen/aktualizován IP adresní plán, stanoveny jmenné konvence apod.
13. bude staven způsob distribuce IP směrovacích záznamů pro interní síť MHMP, pro perimetr MHMP, pro Mepnet lokality

14. budou definovány komunikační pravidla pro nastavení firewallů
15. budou definovány bezpečnostní politiky pro zabezpečení komunikačních linek (IPSec, 802.3ad)
16. budou definovány požadavky na součinnost externích subjektů
17. vytvoření postupu migrace pro stávající zařízení, které budou dále využity (Catalyst 6500, linkové karty, SFP/SFP+ moduly apod.)
18. bude zpracován projekt k vytvoření řešení vizualizace a definice vztahů IT aktiv a služeb organizace, kde výstupem bude řešení v jednotné uživatelské správě přes GUI:
 - o Správa IP adresního plánu organizace
 - o Provoz a podpora služeb DNS a DHCP
 - o Řízení přístupu do sítě v rozsahu nástrojů:
 - o Network Access Control (NAC)
 - o SSL VPN
 - o Monitoring chování sítě pro úroveň L2, L3 a L4
 - o Vizualizace vztahů IT aktiv a provozovaných služeb organizace
 - o Evidence popisných informací IT aktiv pro podporu šetření bezpečnostních událostí
 - o Modelování logických vrstev pro definici vztahů klíčových procesů organizace na IT aktiva
19. bude zpracován projekt k vytvoření kompletní přehled nad síťovým provozem a jeho inteligentní distribuci a předzpracování předtím než dorazí na monitorovací nástroje (např. IPS/IDS, SIEM, DLP, APM, apod.). Dodaným řešením zajištěn přehled nad veškerým síťovým provozem - včetně do fyzických (včetně vzdálených lokalit) i virtuálních sítí.
20. Bude zpracován návrh integrace s ostatními bezpečnostními systémy provozovanými nebo využívanými Zadavatelem, které budou umožňovat napojení na Bezpečné síťové prostředí
 - o Perimetrové firewally společnosti
 - o Systémy řízení a sledování přístupů k sítí, DDI a Network Visibility Module
 - o Systémy aplikačního balancování a ochrany
 - o Systém správy logů z provozní a bezpečnostní infrastruktury
 - o Nástroje pro detekci a vyšetřování kybernetických incidentů
 - o Nástroje pro správu bezpečnostních událostí SIEM
21. Stanovení základních kategorií dat pro směrování do výše uvedených systémů - bezpečnostní log data, log data s vlivem na služby, log data s vlivem na aplikace, log data s vlivem na systémy.
22. Detailní popis implementace, včetně časového harmonogramu
23. Popis instalačních procedur
24. Návrh akceptačních kritérií pro předání díla, včetně návrhu akceptačního protokolu pro předání díla do provozu

Detailní návrh bude podroben interní oponentuře Zadavatele. V případě připomínek Zadavatele je Dodavatel povinen tyto připomínky do detailního návrhu řešení zpracovat.

Akceptace a předání detailního návrhu řešení je nutnou podmínkou pro realizaci dalších etap plnění zakázky. Detailní návrh řešení se stane jeho předáním majetkem Zadavatele, který jej bude moci plně využít pro svoje potřeby ke všem způsobům užití, a to bez dalšího souhlasu zhotovitele nebo zpracovatele.

2. Dodávka technologií Bezpečného síťového prostředí

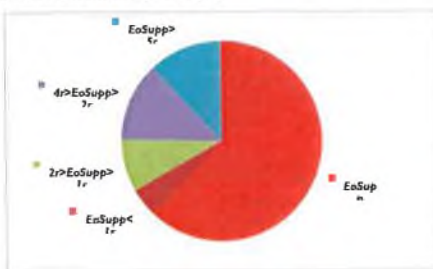
POPIS STÁVAJÍCÍHO STAVU

Infrastruktura MHMP je rozložena ve 21 lokalitách. Centrálními lokalitami jsou lokality DC1 a NUB, které jsou vzájemně propojeny MPLS Interconnect sítí prostřednictvím koncových MPLS zařízení Juniper MX240.

Lokality VAL, STAR, REZ, KLA, MKP, JUN a NR jsou fyzicky připojeny optickými vlákny napřímo (mimo MPLS WAN) na jednu z centrálních lokalit - NUB. Lokality JUN a NR jsou připojeny Single Mode (SM) optikou. Ostatní lokality jsou na centrální lokalitu NUB připojeny Multi Mode optikou (MM). U zbývajících 12 lokalit MHMP (BOH, BREV, BUB, DDM, CHAR, JAR, EMA, KON, OPLET, RAB, RYT, VYS) je konektivita na centrální lokality zajištěna prostřednictvím MPLS sítě WAN, která je připojena do MPLS Interconnect sítě, propojující centrální lokality (DC1 a NUB).

Vnitřní infrastruktura jednotlivých lokalit se typicky liší podle její velikosti. Malé lokality, kterých je většina, jako jsou např. VYS, VAL, STAR, RYT, REZ, OPLET, MKP, CHAR, JAR, BOH jsou vybaveny malým počtem L2 switchů bez zajištěné vysoké dostupnosti (redundance zařízení a fyzických propojů). Centrální lokality DC1, NUB a větší lokality JUN, NR, KON jsou kromě přístupových L2 switchů vybaveny redundantními L3 switchi, které zajišťují L3 routing již v rámci své lokality. Výjimkou je jedna z menších lokalit EMA, která je rovněž vybavena L3 switchem, který zajišťuje pro lokality Inter-VLAN routing. Tento L3 switch ovšem rovněž není v redundantním zapojení pro zajištění vysoké dostupnosti.

Celkový počet stávajících aktivních prvků je 304.



Obrázek 1 Statistika dostupnosti technické podpory od výrobce (EOS)

Z analýzy typů síťových prvků používaných v infrastruktuře MHMP vyplývá, že pro 62% (189ks) zařízení již neexistuje žádná dostupná technická podpora pro případ jakéhokoli problému v hardwaru nebo v software (EoSnp). Další 5% (14ks) zařízení je těsně před koncem dostupnosti podpory resp. podpora bude dostupná již jen několik měsíců (EoSnp<1r). Pro 9% (26ks) zařízení bude podpora k dispozici po dobu kratší než 2 roky (2r>EoSnp<1r). Pro 13% (39 zařízení) zařízení bude technická podpora dostupná po

následující 2 až 4 roky (4r>EoSnp>2r). V případě, že dostupnost technické podpory je kratší než 5 let, to znamená, že již byly dopsány termíny pro morální životnost zařízení (End of Life) a ukončen prodej takových zařízení (End of Sale). Z analýzy používaných zařízení plyne, že 88% (268ks) zařízení je již za hranici své morální životnosti. Pouze v případě 12% (36ks) zařízení z celkového počtu 304 kusů je možné tyto zařízení považovat z hlediska jejich životnosti za vyhovující.

REDUNDANCE

Prakticky v žádné z 21 lokalit není zajištěna potřebná úroveň redundance síťových zařízení a tedy vyhovující vysoká dostupnost (HA).

Ve většině případů lokality neobsahují dvojici redundantních páteřních prvků. Pokud takové prvky v lokalitě existují (např. DC1, NUB, KON), nejsou tyto prvky v HA režimu provozovány. To znamená, že na prvcích, které podporují vytváření stolu switchů, kdy se z více jednotlivých switchů (Catalyst 2960S, 2960X, 3750, 3750X) vytvoří jeden fyzický switch propojený na úrovni vnitřních sběrnic nebo na prvcích, které umožňují propojení prostřednictvím 10Gb rozhraní do virtuálních chassis lze efektivně propojovat s dalšími fyzickými switchi, těchto vlastností nevyužívá (nebo nejsou takové HA vlastnosti na switchích vůbec dostupné). Takové stoly nebo virtuální chassis lze efektivně propojovat s dalšími switchi případně servery prostřednictvím agregovaných (EtherChannel 802.3ad) Ethernet propojů bez nutnosti vytvářet v síti zbytečné smyčky a provozovat, mimo nezbytnou míru, protokol STP (Spanning Tree Protocol), který vyžaduje nedostatečnou konvergenci sítě v případě výpadků a poruch na síti.

Hlavní nedostatky:

- Nedostatečná redundance páteřních nebo centrálních prvků (stack/stoli, VSS).
- Pouze v minimální míře se využívá agregace fyzických propojů do vícenásobných tras (802.3ad).
- Prakticky se nevyužívá agregací (802.3ad) fyzických tras a jejich zapojení do různých prvků jednoho redundantního uzlu (protože takové redundantní uzly neexistují).
- Nevyužívá se rozložení zátěže mezi přenosové trasy a síťové prvky (také z důvodů uvedených v předchozích bodech).
- Riziko výpadků v síti v důsledku poruch nezálohovaných fyzických komponent sítě.
- Riziko výpadků v síti v důsledku pomalé nebo chybové konvergence sítě postavené na STP protokolu.
- V souvislosti s výše uvedenými body vyplývá nemožnost zajištění redundantního napájení klíčových uzlů sítě.

BEZPEČNOST

Hlavní nedostatky:

- Nejednotná koncepce architektury vyplývající z postupné výstavby sítě v dlouhém časovém horizontu.
- Komplikovaná správa takové infrastruktury.
- Z důvodu morální zastaralosti některých klíčových bezpečnostních prvků vyřazeny klíčové bezpečnostní služby.

- Chybějící kontrolér pro řízení přístupu k aplikacím a dělení zátěže na serverové farmy (původní ACE).
- Systém pro monitoring, sběr, korelaci a vyhodnocování bezpečnostních událostí (původní MARS 55).
- Východí brány pro lokální síť jednotlivých lokalit nejsou ve správě MHMP (PE zařízení MPLS sítě WAN).
- Na switchích chybí řízení oprávnění konektivity koncových zařízení k LAN sítím MHMP - chybějící 802.1X.
- Datové přes veřejné MPLS sítě nejsou šifrovány.

Požadavek na cílový stav projektu

- Veškerá stávající zařízení po době morální životnosti budou nahrazena
- Zařízení a komponenty, které vyhovují funkčně a budou v horizontu min. 5 let podporovány výrobcem, budou dále využívány. Tímto způsobem budou maximálně zužitkovány vynaložené investice MHMP
- Z pohledu počtu připojených zařízení nebude v cílovém stavu docházet k zásadnímu navýšení
- V klíčových bodech sítě bude v maximální možné míře použito redundantních mechanismů
- Dojde ke změnám ve prospěch navýšení bezpečnosti přenášenců dat. Tímto lze předejít negativním bezpečnostním nálezům v rámci analýzy rizik (např. v rámci nových legislativních požadavků - GDPR)
- Dojde k zavedení ověřování zařízení připojovaných se k lokální síti
- Budou použity analytické nástroje pro detekci konkrétních aplikací a škodlivého kódu v síťovém provozu
- Bude nasazen nástroj pro centrální řízení a správu síťových politik

Očekávané přínosy řešení

- Bezpečnostní přínosy plynoucí z analýzy síťového provozu:
 - Monitoring bezpečnosti – detekce provozu porušující bezpečnostní politiky, anomálie, šíření škodlivého kódu. Včetně monitoringu každého přenášeného paketu umožňujícího detekovat i útoky vedené proti organizaci.
 - Detekce šíření škodlivého kódu i v šifrovaném provozu, bez porušování utajení provozu šifrou
 - Utajení šifrováním veškerého provozu v infrastruktuře mezi všemi prvky a budovami, zejména v částech sítě, které nejsou fyzicky zabezpečeny nebo jsou snadněji fyzicky přístupná či nejsou zcela pod kontrolou organizace. Vysoce propustnou a bezpečnou technologii IEEE 802.1ae, která však přesto umožňuje plně využívat veškeré síťové funkce zařízení.
- Nezávislost na poskytovateli
 - Vlastní přehledná VPN síť přináší nezávislost na poskytovateli MAN připojení

- Umožňuje rovněž zříditi záložní přípojky u nezávislého poskytovatele

11. Viditelnost aplikací
Zařízení používají vzhled do vyšších vrstev OSI modelu pro rozpoznání přenášené aplikace. Tuto znalost následně využívají při uplatnění bezpečnostních nebo i QoS pravidel podle detekované aplikace. Současné poskytlují i telemetrická data kategorizovaná podle přenášenců aplikací

12. Telemetrie, programovatelnost/automatizace
Pro zjednodušení správy řešení a automatizaci rutinních úkonů obsahují zařízení programovatelná rozhraní jak pro vlastní ovládaní zařízení tak i pro automatizovaný a vysoce škálovatelný (autonomní) sběr požadovaných telemetrických dat

13. Vysoká dostupnost (Modulární OS, patching)
Moderní zařízení s moderní architekturou operačního systému zaměřenou na dosažení vysoké dostupnosti zařízení a jím poskytovaných služeb (dříve dostupnou pouze u zařízení určených pro poskytovatele služeb)

14. SDA Fabric

V řešení použité zařízení umožňují vytvoření tzv. "fabriky", tedy sítě ovládané primárně pomocí politik. Pomocí vyjádření záměru, kterého je potřeba dosáhnout, nikoli konfiguračními změnami konkrétních zařízení. Takový přístup k řízení sítě přináší velmi jednoduchým způsobem vytvořitelnou, vysoce bezpečnou a velmi škálovatelnou segmentaci (bezpečnostní oddělení segmentů, virtualizaci) celé infrastruktury, zabezpečení a řízení přístupu do sítě, monitoring provozních parametrů a telemetrická data. Segmentace je prováděna na základě identity koncového uživatele, nikoli jeho síťových parametrů, což umožňuje vysokou škálovatelnost, flexibilitu i při častých nebo dočas- ných změnách uspořádání koncových uživatelů infrastruktury, jejich mobility. Není potřeba žádný manuální zásah do infrastruktury, a přesto jsou zachovány veškeré politiky všech uživatelů. Telemetrická data z provozu infrastruktury pro jejich analytické zpracování nebo chod relevantních pro primární předmět podnikání společnosti nebo chod organizace. Obecně tento přístup zefektivňuje zavádění nových služeb infrastruktury a řešení problémů a úkolů.

Předpokládá se využití filosofického směru, který byl v prostředí MHMP zvolen v nových DC (např. DC4, DC2). Jedná se o technologii SDN – software defined network. V tomto prostředí již datové toky nejsou za všech okolností řízeny tradičním způsobem, ale mohou být ovládaný softwarově na základě schopnost specificky zacházet s provozem dle příslušnosti k jednotlivým aplikacím.

Seznam technologických celků dodávky Bezpečné síťové prostředí

Předpokládáné rozdělení objemu dodávky v jednotlivých kusů, dle Přílohy č. 5; Podrobná specifikace ceny, Smlouvy, na jednotlivé fáze.

Součástí Detailního návrhu řešení může být úprava množství technologií, dodaného v jednotlivých fázích, avšak celkový počet technologií nesmí být pozměněn.

Technologie	Fáze 1	Fáze 2
- Bezpečné rozhraní pro analýzu síťového provozu	0	4
- Bezpečnostní hraniční brány firewall pro síť Mepnet	5	0
- Centrální kontrolér LAN sítě	3	0
- Monitorování datových toků	0	1
- Řízení přístupu k síťovým prostředkům (802.1x)	2	2
- Správa síťového prostředí	0	1
- Datacentrové řešení Spine-Leaf	1	0
- Spine vrstva	2	0
- Leaf vrstva – 10GB SFP+	4	0
- Leaf vrstva 10GB – RJ45	2	0
- Leaf vrstva 1GB – RJ45	10	0
- Next-Generation Firewall	2	0
- Virtuální privátní síť, vzdálené přístupy do sítě	5300	0
- Přístupové přepínače s 24 PoE porty	30	50
- Distribuční přepínače	30	43
- Přístupové přepínače s 48 PoE porty	32	40
- Centrální přepínače	3	3
- Agregční směrovač	0	2
- Hraniční pobočkové směrovače	4	2
- Rozšiřující 10GB karty	3	0
- Rozšiřující servisní moduly	4	0
- Propojovací moduly	200	143

Podrobné specifikace a parametry technologií jsou popsány v následující kapitole této přílohy ZD

Pravidla pro vyplňování technických parametrů řešení

Uchazeč vyplní v následujících kapitolách pouze všechny žlutě označené části.

Tato příloha slouží k uvedení názvu / typu a počtu konkrétního nabízeného řešení či zařízení a dále k vymezení minimálních technických požadavků zadavatele na řešení a osvědčení jejich splnění uchazečem. Požadavky zadavatele jsou uvedeny ve sloupci „Parameter“ nebo „Požadovaná hodnota parametru“.

Následná smlouva s vybraným uchazečem může být v této části upravena tak, aby obsahovala již pouze uchazečem nabídnuté zařízení a jeho technické parametry.

V níže uvedených tabulkách jsou uvedeny veškeré povinné minimální parametry kladené na celý systém. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.

Dodavatel v níže uvedených tabulkách vyplní sloupce „Splňuje ANO/NE“ a pokud je požadován i „Popis jak bude požadavek splněn/řešen“.

Sloupec „vyjádření „Splňuje ANO/NE“ může nabývat pouze hodnot ANO nebo NE, bude-li uvedeno něco jiného, je to rovněž důvod k vyřazení nabídky.

Sloupec „Nabízená hodnota (Popis)“ bude obsahovat podrobný popis, jak dodavatel požadavek naplní.

Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek i to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky stanovené Zadavatelem.

Výše uvedená pravidla na vyplnění tabulek jsou společná pro všechny kapitoly této přílohy ZD.

2.1. Bezpečné rozhraní pro analýzu síťového provozu

Technické požadavky na řešení garantovaného a bezpečného rozhraní pro analýzu síťového provozu.

Systém musí poskytovat funkcionality umožňující vytvoření bezpečného rozhraní mezi síťovými prvky nové infrastruktury DC MHMP a provozně bezpečnostními nástroji, které vyžadují čtení kopírovaného síťového provozu. Takto vytvořené bezpečné předávací rozhraní (jinými slovy integrační platforma pro síť – neboli packet broker) bude sloužit k předávání informací o síti a se sítě, které bude možno bezpečně a bez dalších nároků na síť (tedy bez ohrožení její stability) využít v nástrojích třetích stran.

Zdroje dat k monitoringu je třeba zajistit také z virtualizační platformy VMware, tedy z virtuálních síťových přepínačů, které jsou zajištěny na úrovni hypervizoru virtuálního prostředí.

Předávací rozhraní síťového provozu musí být dále vybaveno možnostmi manipulace s předávanými informacemi, čímž bude umožněno např. filtrování vybraného typu provozu k odeslání do zařízení třetích stran, nebo maskování citlivého obsahu, aby nemohlo dojít k jeho vyzaření a neoprávněnému nakládání.

Minimálně je požadováno poskytnutí těchto parametrů a pokrytí těchto oblastí:

- Schopnost připojit dodávané řešení až na 40 x 10GE optických rozhraní, nebo až na 40 x 10GE optických rozhraní
- Schopnost připojit dodávané řešení až na 40 x 1GE RJ45 metalických rozhraní, nebo až na 40 x 1GE optických rozhraní
- Schopnost připojit dodávané řešení až na 2 x 40GE optických rozhraní, nebo až na 2 x 100GE optických rozhraní
- Schopnost agregovat a zpracovat celkem 100 Gbps síťového provozu
- Podpora těchto způsobů integrace s monitorovanou sítí:
 - o SPAN/MIRROR port – připojení na optické či metalické rozhraní síťových přepínačů, které jsou nastaveny do režimu duplikace provozu pro monitoring
 - o Možnost rozšíření řešení o režim TAP – síťový rozbočovač pro optické a metalické sítě
- Agregace provozu z více zdrojů do jednoho výstupního rozhraní a média
- Podpora sledování síťového provozu ze síťového přepínače hypervizoru VMware
- Schopnost sledovat provoz v 10 serverech VMware virtuálního prostředí HMP
- Možnost řízení pravidel směrování monitorovaného provozu, kde je možné libovolným odběrným místům přidělit konkrétní zdrojová data ze sledovaného síťového provozu
- Možnost manipulace s daty z monitorovaného provozu, předtím než dojde k jejich předání odběrnému místu
- Možnost deduplikovat a optimalizovat provoz předávaný odběrným místům

- o Možnost předávat unikátní informace i přesto, že na vstupu přichází z několika zdrojů současně (deduplikace)
- o Možnost předávat omezené informace o síťovém provozu: jen NetFlow, nebo jen hlavičky provozu bez obsahu
- o Možnost upravovat výstupní data obohacením o dodatečné informace

Tabulka detailních požadavků na dodávané řešení garantovaného a bezpečného rozhraní pro analýzu síťového provozu:

Základní údaje	Nabízená hodnota
Výrobce zařízení	Digitální
Počet kusů zařízení - 4	*
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uveďte Uchazeč hlavní produktové číslo nabízeného zařízení)	OVS-HC2m OVS-TA3m
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v češtině nebo anglickém jazyce	https://www.digitall.com/templ/34m/resources/library/english/data-sheet/ds-aggregate-ovs.pdf https://www.digitall.com/templ/34m/resources/library/english/data-sheet/ds-aggregate-series-ovs-hc2m-ovs-ta3m.pdf

Parametr	Požadovaná hodnota parametru (pro jedno fyzické zařízení)	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Integrace s monitorovaným síťovým prostředím	Analýza síťového provozu probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly a monitorovány jsou tedy všechny probíhající spojení na všech síťových portech monitorované infrastruktury.	Technologie analyzuje veškerý provoz a připojených rozhraní sítě a proto disponuje dostatečným množstvím a kapacitou vstupních síťových rozhraní. Technologie nerozlišuje provoz na vstupních rozhraních a zpracovává veškerá zasláná data.	ANO

Integrace s monitorovaným síťovým prostředím	Integrace se síťovým prostředím je zajištěna zrcadlením síťovým provozem, který Zadavatel poskytne na vyhrazených portech přepínačů svých DC.	Data jsou primárně do nabízené technologie síťová ze SPAN rozhraní monitorované síťové infrastruktury. Přičemž SPAN porty zajišťují síťové prostředí rákosníka.	ANO
Integrace s monitorovaným síťovým prostředím	Pro integraci s monitorovanou sítí bude možné použít kombinaci metalických a optických síťových rozhraní DC Zadavatele.	Navrhované řešení disponuje kombinací rozhraní 1Gbps metalické a 10, 40Gbps optické.	ANO
Integrace s monitorovaným síťovým prostředím	Bude možné rozšířit řešení o in-line způsobu zapojení pro metalické i optické komunikační trasy pomocí TAP	Nabízené řešení je možné rozšířit o specifické moduly TAP, které jsou po přizpůsobení plně integrovatelné. Výrobce disponuje TAPy metalickými i optickými.	ANO
Integrace s monitorovaným síťovým prostředím	Nabízené řešení bude agregovat provoz z dvou DC HMP a bude jej předávat v definovaných výstupních rozhraních v libovolné lokalitě (monitorovaný provoz tak může být tunován mezi lokalitami).	Nabízené řešení je koncipováno jako dva páry technologií (vždy jedna dvojice do každé lokality) a dokáže vstupní síťový	ANO

Integrace s monitorovaným síťovým prostředím	Výstupní rozhraní budou typem média nezávislé na vstupních rozhraních monitorované sítě.	provoz protnelovat vždy do druhé lokality.	ANO
Integrace s monitorovaným síťovým prostředím	Bude podporováno sledování provozu z virtuálního síťového přepínače virtualizační platformy VMware. Cílem je získat jednotný obraz chování sítě, včetně komunikací uvnitř virtuální platformy.	Nabízené řešení slouží pro konverzi a unifikaci médií. Výstupní rozhraní nejsou typem a rychlostí závislé na vstupních rozhraních.	ANO
Integrace s monitorovaným síťovým prostředím	Dodávané řešení bude schopno zpracovat síťový provoz o celkové kapacitě alespoň 100Gbps (údaj před optimalizací a filtrací).	Sečtení nabízeného řešení jsou licenze pro pokrytí toti serverů pro virtualizaci pro zajištění plného vzhledu do síťového provozu uvnitř hypervizorů.	ANO
Integrace s monitorovaným síťovým prostředím	Počet vstupních rozhraní dodávaného řešení určených k integraci s monitorovanou sítí bude minimálně 20 v každém ze dvou DC HMP	Processorový výkon nabízeného řešení pro zpracování vstupních dat je schopen pracovat se síťovým provozem až 800Gbps.	ANO

Filtrování a manipulace s monitorovaným provozem	Možnost provádět filtrování síťového provozu před jeho předáním na výstupní rozhraní pro připojení analytických nástrojů. Cílem je umožnit předat jen potřebné typy komunikací pro každý připojený analytický nástroj.	4 x 40Gbps Součástí nabízeného řešení je licenze na filtrování obsahu provozu pro pokrytí požadované funkcionality.	ANO
Filtrování a manipulace s monitorovaným provozem	Pravidla pro filtrování provozu musejí být definovatelná podle 4. vrstvy ISO/OSI modelu.	Filtrování dle L4 pravidel.	ANO
Filtrování a manipulace s monitorovaným provozem	Možnost provádět manipulace s provozem do monitorovacích zařízení: - Maskování citlivých informací – umožní bezpečnostním týmům skryt citlivé informace a tím ochránit organizaci před porušením nařízení plynoucích z ZákB popř. GDPR. - Předávání jen vybrané části komunikací, které jsou předmětem zájmu připojeného monitorovacího zařízení - předávání jen hlaviček provozu bez obsahu paketů. - Doplňování dodatečných informací o zdroji monitorovaných dat pro lepší orientaci a obohacení monitoringu.	Součástí nabízeného řešení je licenze na manipulaci s obsahem provozu pro pokrytí požadované funkcionality.	ANO
Filtrování a manipulace s monitorovaným provozem	Potřebné komponenty pro sledování virtuálního prostředí budou dostupné ve formátu OVA/OVF template.	Dle požadavku.	ANO
Filtrování a manipulace s monitorovaným provozem	Monitorovaný provoz u lokality jednoho DC může být v některých případech potřeba předat do výstupních rozhraní v druhém DC. Řešení tedy musí umět tunelovat provoz mezi lokalitami.	Advanced Tunneling feature je součástí nabízeného řešení.	ANO
Filtrování a manipulace s monitorovaným provozem	Monitorovaný provoz musí být v dodávaném řešení optimalizován: - Deduplikován - Odstranění nadbytečných údajů - Obohacen o metadata	De-Duplication feature je součástí	ANO

Správa a ovládání komponent dodávaného řešení	Možnost spravovat jednotlivé komponenty pomocí bezpečného rozhraní SSH nebo HTTPS.	nabízeného řešení.	ANO
Správa a ovládání komponent dodávaného řešení	Možnost napojení zařízení na SIEM z důvodu monitoringu administrátorských aktivit.	Obě požadované varianty jsou podporovány.	ANO
Správa a ovládání komponent dodávaného řešení	Generování statistik o sledovaném síťovém provozu na všech vstupních síťových rozhraních.	Technologie loguje přístupy a logy je možné načíst ve formátu SYSLOG na technologii 3. stran.	ANO

2.2. Bezpečnostní hraniční brány firewall pro síť Mepnet

Bezpečnostní hraniční brány firewall pro vybraných X organizací připojených do metropolitní sítě Mepnet, jehož primárním určením je ochrana vstupního rozhraní do sítě a garance čistoty provozu. Brány budou zařazeny do společného centrálního nástroje pro správu bezpečnostní politiky MHMP a Mepnet, který je provozován na technologii Check Point.

Metropolitní síť (Mepnet), která propojuje organizace a subjekty zřízené Hlavním městem Prahou, představuje pro bezpečnost opravdovou výzvu, neboť propojuje subjekty s rozdílnou úrovní řešení vlastní bezpečnosti. Z tohoto důvodu a pro ochranu společné sítě Mepnet je požadováno dodání hraničních bran firewall, které zajistí bezpečnost vybraných přípojných míst do sítě Mepnet. Pro iniciační fázi zabezpečení bylo vybráno 5 městských organizací.

Pro jednotlivé připojené lokality je požadováno řešení, které umožní nejen ochranu přístupu do sítě mepnet, ale bude umožněno realizovat na stejném systému komplexní perimetrou ochrany připojené lokality.

Základní údaje	Nabízená hodnota
Výrobce zařízení	Check Point
Počet kusů zařízení - 5	5
Produktové číslo (typ) nabízeného zařízení (v případě, že je k dispozici popisná více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	CPAP/SOP/m-NGTS

Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce

<https://www.cisco.com/c/en/us/products/routers/4848series/4848-5400-series.html>

Parametr	Požadovaná hodnota parametru (pro jedno fyzické zařízení)	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Požadavky na HW bezpečnostní brány firewall	<ul style="list-style-type: none"> Brána bude provozována na vlastním HW Parametry pro umístění do DC: <ul style="list-style-type: none"> Rozměr pro umístění v RACK do 2U Redundantní napájení 2x230V Zařízení bude vybaveno out-of-band management rozhraním Rozhraní pro síťová připojení: <ul style="list-style-type: none"> 8 x RJ45 10/100/1000 Možnost rozšíření o 10GbE fiber Podpora 802.1Q, port teaming, LACP, DHCP server/relay Možnost řízení QoS pro jednotlivé realizované komunikace (i pro šifrovaný provoz) 	Nabízené zařízení je dodáváno jako vlastní HW platforma (appliance) požadovaných rozměrů a s osazením dle požadovaných parametrů. Nezávislý management interface je součástí nabízeného řešení.	ANO
Požadavky na výkon zařízení	<p>Propustnost systému firewall při řízení síťových komunikací:</p> <ul style="list-style-type: none"> 10 Gbps <p>Minimální garantovaná propustnost systému při plné inspekci provozu (FW, IPS, URL filtering, IP reputation, VPN, Antivirus, Sandbox):</p> <ul style="list-style-type: none"> 350 Mbps <p>Propustnost systému při plné inspekci provozu (FW a IPS):</p> <ul style="list-style-type: none"> 1 Gbps <p>Propustnost provozu při šifrování AES-128 (bez inspekce):</p> <ul style="list-style-type: none"> 2 Gbps <p>V lokalitě bude od dodaného řešení vyžadována ochrana celého perimetru s vlastní internetovou přípojkou.</p> <p>V lokalitě bude od dodaného řešení vyžadována ochrana intra DMZ provozu.</p>	Všechny požadované propustnosti jsou výrobcem deklarované a nabízené řešení je splňuje bez výhrad. Přehled parametrů (real-world): FW až 10Gbps FULL 395 Mbps IPS až 1Gbps AES-128 2Gbps	ANO

Tabulka společných detailních funkčních požadavků na dodávané řešení hraničních bran firewall pro vybrané lokality:

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Centrální management síťové bezpečnosti	<p>Dodávané řešení musí být plně kompatibilní se stávajícím nástrojem pro správu síťové bezpečnosti politiky provozovaném na platformě Check Point.</p> <p>Integrace musí být zajištěna na úrovni:</p> <ul style="list-style-type: none"> Správa bezpečnostní politiky Centralizace logů z bezpečnostní brány firewall Monitoring životních funkcí brány firewall i všech statistik o komunikacích a bezpečnostních událostech Konfigurace síťových parametrů brány firewall Správa licencí a subscriptions Ovládání stavu brány firewall (aktivní, vypnutá) 	Řešení je plně kompatibilní s management prostředím Check Point a nabízené brány je tak možno integrovat do současného systému správy bezpečnostní politiky.	ANO
Centrální management síťové bezpečnosti	Dodávané řešení umožní pro potřeby jednotlivých připojených lokalit definovat specifické sady bezpečnostních pravidel a umožní vlastní přístup skupiny administrátorů k této politice. Bude tak podporován tzv. více-doménový režim správy politik.	Nabízené bránové řešení je plně podrobitelné centrální správě tzv. MDM managementu, pokud tento bude provozován v prostředí MHMP.	ANO
Centrální management síťové bezpečnosti	Správa logů bude opět řešena pro jednotlivé připojené lokality zvlášť, aby nedocházelo k sdílení logů mezi správci z jednotlivých přípojních míst.	Nabízené bránové řešení je plně podrobitelné centrální správě logů v prostředí jednotného managementu MHMP.	ANO

Požadavky na bezpečnostní funkce dodané brány firewall	<ul style="list-style-type: none"> Firewall VPN (šifrování provozu site-to-site) Intrusion Prevention System URL filtering Řízení provozu aplikací včetně jejich automatického rozpoznávání Ochrana proti přístupu na známé nebezpečné cíle (např. C&C) Sandbox ochrana před útoky typu oday <p>Pro všechny bezpečnostní funkce bude aktivní podpora výrobce obsahující aktualizaci definic a vzorků.</p> <p>Jednotlivé funkcionality budou umožňovat detailní řízení pravidel pro jejich uplatnění v síťovém provozu.</p>	Součástí nabízeného řešení je plně podpora Next Generation Threat Prevention & SandBlast a to včetně 3 roků předplatného pro definice výrobce. Podpora výrobce: Premium Collaborative Enterprise Support	ANO
--	---	--	-----

2.3. Centrální kontrolér LAN sítě

Centrální kontrolér slouží jako nosič modulární platformy, která umožňuje vytvářet virtualizované prostředí nad LAN sítěmi, které umožňují automatizovaný provoz LAN aktivních prvků, které sdružuje do řízených skupin. Síťové prvky obsažené v řízené skupině se již nekonfigurují ručně, ale přes rozhraní modulární platformy. Jednotlivé řízené skupiny můžou být geograficky oddělené avšak s IP konektivitou na centrální kontrolér.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 3	3
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uveďte Uchazez hlavní produktové číslo nabízeného zařízení)	DNA-15W-APL
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html
Požadovaná hodnota parametru	Mínimální požadavky Splněno (ANO/NE)
Řízení celého řešení	Centrální kontrolér ANO
Funkce pro zcela automatické sestavení a konfiguraci fyzické infrastruktury	ANO
Veškeré síťové politiky jsou implementovány prostřednictvím centrálního kontroléru	ANO

Podpora vytváření multi-tenant prostředí - členění koncových uživatelů a zařízení do oddělených virtuálních sítí	ANO
Podpora mikrosegmentace - členění koncových uživatelů a zařízení do logických skupin podle jejich role, nezávisle na IP adresaci koncových zařízení a síťové topologii	ANO
Podpora funkcionality distribuované default gateway na jednotlivých edge přechátech	ANO
Podpora mobility uživatelů a zařízení přes jednotnou infrastrukturu bez nutnosti vytvářet Le broadcast domény	ANO
Integrace WLAN infrastruktury s možností terminovat datový provoz od bezdrátově připojených uživatelů přímo na edge přechátech	ANO
Společné politiky pro pevně i bezdrátově připojené uživatele	ANO
Centralizovaná definice pravidel pro řízení přístupu uživatelů a zařízení v síti	ANO
Podpora real time telemetrie, schopnost monitorovat každý paket, každý datový tok procházející infrastrukturou	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v10 nebo IPFIX	ANO
Požadovaná funkcionality centrálního kontroléru	
Formát zařízení	HW appliance ANO
Typ zařízení	SDN kontrolér ANO
Redundantní nasazení	ANO
Grafické uživatelské rozhraní součástí řešení	ANO
Přístupová práva založená na uživatelských rolích	ANO
Otevřené API rozhraní pro integraci s externími systémy	ANO
Dokumentované API rozhraní pro volání všech dostupných funkcí kontroléru	ANO
Pokročilá správa operačního systému síťových zařízení	
<input type="checkbox"/> Patching management	ANO
<input type="checkbox"/> SW Image Rollback	
<input type="checkbox"/> Verifkace integrity SW image	
Inventarizace nasazeného HW	ANO
Hierarchické zobrazení topologické mapy včetně jejího členění na jednotlivé lokality	ANO

GUI rozhraní pro detailní přehled o výkonnosti a stavu celé komunikační infrastruktury včetně monitorování stavu jednotlivých zařízení (využití CPU, DRAM (má být jednotlivých síťových rozhraní atd.)		ANO
Konfigurace sítě a síťových politik (rozdělnictvím, definovanými workflows)		ANO
Podpora mikrosegmentace - členění koncových uživatelů a zařízení do logických skupin podle jeho identity. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky (bezpečnostní politiky) vůči jiným skupinám		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění - tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimě 8x5xNBD tuto záruku eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému popř. požadovaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být odkaz výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude naděšitelná pochopnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.4. Monitorování datových toků

Nástroj pro monitorování sítě s primárním zaměřením na identifikaci bezpečnostních incidentů. S použitím NetFlow a Advanced Security analyzuje i šifrovanou komunikaci a dokáže porovnat síťový provoz proti databázi bezpečnostních hrozeb udržovanou výrobcem. Obranný perimetr se tak posouvá na síťovou vrstvu, kde je umožněno zachytávat hrozby i pro antivirovémi programy nevybavené zařízení jakou jsou IP Telefony, CCTV kamery apod. Používá NetFlow záznamy shromážděné z exportu od všech připojených zařízeních v síti. Systém shromažďuje informace Netflow, IPFIX, sFlow, stejně jako ekvivalenty třetích stran (jFlow). Korelace těchto informací společně umožňuje nahlédnout na zdrojovou a cílovou adresu, zdrojový a cílový port, rozhraní, IP TOS, IP protokoly, Next Hop IP, TCP značky, stejně jako na informace L7 aplikací pomocí flowsensorů.

□ Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet setů zařízení: Management 1ks, Collector 1ks, UDF replikátor 2ks	4ks odvoz	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uveďte Uchazeč hlavní produktové číslo nabízeného zařízení)	87.881Cazen-Ry	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html	
Požadovaná hodnota parametru	Minimální požadavky	Společně (ANO/NE)
Formát zařízení	HW appliance	ANO
Centrální správa appliance (kolektorů, senzorů, atd.) pro sběr a analýzu dat, případně dalších komponent systému, distribuovaných v síti		ANO
Možnost sběru dat/integrace s dalšími bezpečnostními prvky a systémy (firewall, web proxy, IDS/IPS, systémy řízení přístupu do sítě, ...)		ANO
Sběr dat a jejich prezentace z velkého množství rozdílných síťových segmentů současně (z distribuovaných appliance)		ANO
Vizibilita napříč pevnými i virtuálními prostředím		ANO
Detekce a prioritizace bezpečnostních hrozeb		ANO
Detekce porušení požadovaných politik		ANO
Dostatečně pokročilé detekční techniky a detailní vzhled do komunikační infrastruktury, aby byl využitelný pro detekci a obranu proti "Advanced Persistent Threats", malware, vříd, síťových červů, cílených útoků, detekci DDoS útoků		ANO
Různé skupiny oznámení (alarmů)		ANO

Přehledové zobrazení všech oznámení (alarmů) na hlavní monitorovací obrazovce		ANO
Seskupování a grafická reprezentace vztahů a toků mezi logickými skupinami (definovanými uživatelem) komunikační infrastruktury		ANO
Historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu		ANO
Napojení na centrální databázi hrozeb poskytovanou výrobcem, která je neustále aktualizovaná		ANO
Integrace se systémem řízení přístupu do sítě pro provádění automatizovaných nápravných akcí		ANO
Integrace se SIEM systémy, minimálně ArcSight a Splunk		ANO
Funkcionality dostupné i pomocí REST API		ANO
Implementace rozhraní pro sdílení informací s jinými bezpečnostními systémy - psGrid nebo draft-ietf-mile-icmp-rid-02		ANO
Přístup administrátorů/uživatelů k systému podle uživatelských rolí /úřadových úřadů		ANO
Appliance pro analýzu a kolektování dat z transportních zařízení		ANO
Sběr dat o datových tocích ze síťových zařízení		ANO
Baselining běžného provozu		ANO
Detekce anomálií oproti běžnému provozu i na L7		ANO
Detekce anomálií na základě toků v síti		ANO
Deduplikace záznamů o toku, pokud byl tentýž tok sebrán z více zařízení v síti		ANO
Spojení všech záznamů o toku, pokud se týkají té samé transakce mezi koncovými zařízeními, včetně zařízení z veřejného Internetu		ANO
Historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu		ANO
Schopnost obohatit záznam toků o URL nebo uživatelskou identifikaci		ANO
Detekce úniku dat z organizace (Data Hoarding, Data Exfiltration)		ANO
Detekce šíření Malware		ANO
Detekce Botnetů		ANO
Detekce DDoS		ANO
Detekce scam sítě		ANO
Min. počet spravovaných appliance pro sběr a analýzu dat distribuovaných v síti	25	ANO
Min. kapacita databáze pro historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu	2 TB	ANO
Minimální počet zpracovaných toků za vteřinu (FPS, Flows per second)	1200000	ANO

Minimální počet síťových zařízení exportujících do jedné appliance pro sběr dat	20000	20000
Minimální kapacita databáze pro historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu	4 TB	ANO
Možnost sbírat a analyzovat agregované FPS (flow per second)	6 mil. FPS	ANO
Licence pro monitorování FPS (flow per second)	15000 FPS	ANO
Licence pro monitorování koncových bodů po minimální dobu 5 let	5000	ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění - tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimě 8x5xNBD tuto záruku eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému popř. požadovaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být odkaz výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude naděšitelná pochopnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.5. Řízení přístupu k síťovým prostředkům (802.1x)

Řešení integruje funkcionalitu univerzálního autentizačního a autorizačního systému s jednotnou správou. Produkt je zaměřený na zjištění a prověření stavu koncových stanic, které se přikládají do sítě (LAN, W-LAN, VPN). Centralizované řešení pro kontrolu přístupu do sítě dokáže ověřit, zda stanice, které se připojují do sítě, vyhovují bezpečnostním pravidlům stanoveným v organizaci.

Univerzální integrační platforma je rozhraní s otevřenou podporou více výrobců, síťových prvků nebo systémů. Umožňuje spolupráci mezi různými platformami IT infrastruktury, jako jsou platformy pro monitorování bezpečnosti, detekční systémy, platformy na definici

síťových bezpečnostních politik, správu zařízení a konfigurace, správu přístupu do sítě a identity uživatele.

□ Základní údaje	Nabízená hodnota	
Výrobce zařazení	CISCO	
Počet kusů zařízení - 4	4	
Produktové číslo (typ nabízeného zařízení (v případě, že je zařízení popisováno více produktovými čísly, uveďte Uchazeč hlavní produktové číslo nabízeného zařízení))	SW-5925-K9	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/Security/identity-services-engine/index.html	
Požadovaná hodnota parametru	Minimální požadavky	Splněno (ANO/NE)
Obecná charakteristika ověřovacího řešení	ANO	
Centralizovaný systém pro ověřování uživatelů, nebo koncových zařízení, Klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.)	ANO	ANO
Formát zařízení	HW appliance	ANO
CPU	8 vCPU	ANO
Paměť	64GB	ANO
Disková kapacita	2,4 TB, RAID 10	ANO
Disková propustnost (I/O Speed)	300 MBps	ANO
počet připojených koncových uživatelů	20000	ANO
Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídicími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové WiFi síti (metodou 802.1x) a pro VPN přístupu		ANO
V rámci ekosystému vytvořenému pomocí integrační platformy musí být možno použít adaptivní řízení síťových prvků organizace, které umožňuje rychle reagovat na útoky metodou přímého využití sítě jako výsuvového prostředku (konkrétní scénáře odpojení uživatele). V praxi toto může znamenat odpojení problematického koncového zařízení přímo od rozhraní LAN přepínače nebo od WiFi přístupového prvku na základě signalizace od detekčního bezpečnostního systému umístěného vnitřní síti.		ANO
Integrace s NGFW, kde nástroj pro kontrolu přístupu do sítě na základě sdílených informací může infikované koncové zařízení pozorovat, omezit jim přístup, nebo napomoci v remediálním procesu		ANO
Poskytuje AAA funkce (viz níže)		ANO

Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)		ANO
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity		ANO
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace		ANO
Je dostupné ve formě Appliance (hardwaru i softwaru)		ANO
Je dostupné ve formě Virtuálního stroje na platformách ESX nebo ESXi		ANO
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)		ANO
Podporované protokoly		ANO
RADIUS pro autentizaci, autorizaci a accounting		ANO
proxy funkce pro externí RADIUS		ANO
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST, EAP-FAST s podporou EAP-Chaining		ANO
Podporované databáze uživatelů (s možností definovat pořadí autentizace		ANO
Interní (pro uživatele i koncová zařízení)		ANO
Active Directory		ANO
Active Directory – více nezávislých domén		ANO
LDAP (RFC 2251)		ANO
RADIUS Token identity source (RFC 2865)		ANO
RSA RADIUS token server		ANO
Autentizace pomocí údajů obsažených v uživatelském certifikátu		ANO
Ověřování uživatelů a zařízení		ANO
Ověření uživatelů heslem nebo certifikátem		ANO
Ověření MAC adresou připojovaného zařízení		ANO
Rozpoznávání typu koncových zařízení a jejich stavu		ANO
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou		ANO
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)		ANO
Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat		ANO
<input type="checkbox"/> Instalovaný operační systém (Windows 7/10)		ANO
<input type="checkbox"/> Opravy instalované v operačním systému		ANO
<input type="checkbox"/> Verze instalovaných programů		ANO

<input type="checkbox"/> hodnoty položek v registry databází systémů		ANO
Windows		
<input type="checkbox"/> Ostav aplikací, zejména antivirů		ANO
Autorizace: flexibilní systém pro definici pravidel pro přístup k síti		ANO
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle		ANO
<input type="checkbox"/> uživatele (role, skupiny),		ANO
<input type="checkbox"/> Ostavu a typu koncového zařízení (viz výše),		ANO
<input type="checkbox"/> místa připojení,		ANO
<input type="checkbox"/> historie připojení		ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě		ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě		ANO
Podpora Change of Authorization (CoA, RFC 3576)		ANO
Možnost jednoduše identifikovat/označit přešlášená data uživatele (rámce) v chráněné oblasti		ANO
Spolupráce na uvedení stanic do požadovaného stavu (informaci, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souborů)		ANO
Accounting		ANO
Zaznamenávání aktivity uživatelů a zařízení připojených k síti		ANO
Dotazovací systém, korelace záznamů, centralizované výkazy		ANO
Systém pro sledování výstrah (úspěšná/nespěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)		ANO
Funcke GUEST serveru		ANO
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fyzických LAN i WiFi		ANO
Oprávnění přidělována správcem přístupu přes portál pro snadné vytváření dočasných účtů		ANO
Samobslužný portál pro uživatele		ANO
Ověření přes HTTP a HTTPS		ANO
Rozhraní pro integraci s externími operátory pro zaslání SMS zpráv s autentizačními údaji		ANO
Další vlastnosti		ANO
Aktivace síťových MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)		ANO
Integrace s MDM systémy		ANO
Možnost vyřazení informací o uživateli z Active Directory (Passive Fingerprint)		ANO
Funcke pro správu ověřovacího systému		ANO
Centralizovaná správa		ANO

Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému		ANO
Zjednodušení správy vytváření skupin uživatelů, koncových a síťových zařízení		ANO
Grafické rozhraní pro definici pravidel přístupu k síti		ANO
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů		ANO
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)		ANO
Zaznamenávání událostí na externí syslog server		ANO
NTP pro synchronizaci času		ANO
SMTP pro zaslání zpráv a výstrah přes e-mail		ANO
Řízení přístupu na síťová zařízení		ANO
Podpora protokolu TACACS+ pro možnost řízení přístupu administrátorů na síťová zařízení		ANO
Proxy TACACS+		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimě RMA/RBD tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému popláváných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.6. Správa síťových prostředí

Komplexní řešení pro správu, vizualizaci a monitorování sítě z jednoho grafického rozhraní. Řešení zajišťuje viditelnost sítě a aplikací, zálohy konfigurací, zjednodušení nasazení a správy zařízení.

☐ Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 1	1ks	
Produktový číslo (typ nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uveďte lhažec hlavní produktové číslo nabízeného zařízení)	PI-UCS-A2L-9s	
Odkaz na www stránce výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html	
Požadovaná hodnota parametru	Minimální Požadavky	Splněno (ANO/NE)
Dostupné v provedení připraveného virtuálního stroje do virtualizovaného prostředí		ANO
Dostupné v provedení fyzické appliance (samostatné zařízení)		ANO
Formát zařízení	HW appliance	ANO
CPU	10 vCPU	ANO
Paměť	64 GB	ANO
Disková kapacita SSD	3,6 TB, RAID 10	ANO
Disková propustnost (I/O Speed)	550 MBps	ANO
Události zpracovaných za jednu sekundu celkem	939	ANO
Syslog zpráv zpracovaných za jednu sekundu	550	ANO
SNMP trapů zpracovaných za jednu sekundu	280	ANO
Systémových událostí zpracovaných za jednu sekundu	80	ANO
Zpracovaných toků Netflow - Netflow flow za sekundu	20000	ANO
Volitelné navýšení počtu zpracovaných toků Netflow - Netflow flow za sekundu	300	ANO
Podpora funkcí pro kontrolu konfigurací na souladu s doporučenými konfiguracemi (best practices)		ANO
Podpora funkcí pro kontrolu přítomnosti známých bezpečnostních chyb v nahrazeném SW spravované sítě infrastruktury		ANO
Podpora funkcí pro kontrolu mílníků HW a SW spravované sítě infrastruktury - zajištění zdraví sítě (konce podpory HW, SW apod.)		ANO
Platforma		ANO
Bezpečný přístup prostřednictvím webového grafického uživatelského rozhraní		ANO
Podpora autorizace a autentizace přístupu do systému vůči TACACS+		ANO

Podpora autorizace a autentizace přístupu do systému vůči RADIUS		ANO
Podpora řízení přístupu ke GUI pomocí identity (SSO - Single Sign On)		ANO
Podpora různých úrovní oprávnění pro přístup do systému (RBAC)		ANO
Podpora multi - uživatelského prostředí GUI s možností využít jak předdefinované skupiny, tak s možností definovat vlastní přístupová oprávnění k funkcím GUI pro alespoň dvě uživatelské skupiny		ANO
Podpora přístupu ke GUI z mobilních zařízení, např. tabletů		ANO
Podpora logování aktivity uživatelů a logování systémových událostí		ANO
Podpora zálohování systému a obnovy ze zálohy		ANO
Možnost redundance pro zajištění vysoké dostupnosti, automatická synchronizace		ANO
Možnost změnit nastavení doby ukládání historických a archivovaných dat		ANO
Možnost omezit přístup uživatelům pouze ke skupině zařízení, např. na základě lokality, typu zařízení apod.		ANO
Možnost monitoringu provozních parametrů aplikací		ANO
Možnost zpracování informací o provozu v síti (NetFlow) včetně deduplikace dat z více zdrojů		ANO
Možnost zobrazit informace o chování aplikací v síti (statistiky, identifikace případných problémů na síťové nebo aplikační úrovni, zhoršení uživatelské zkušenosti uživatelů)		ANO
Podpora protokolu IPv4		ANO
Podpora protokolu IPv6		ANO
Podpora protokolu SSH		ANO
Podpora protokolů SNMPv1, SNMPv2, SNMPv2c a SNMPv3		ANO
Podpora zpracování SYSLOG zpráv		ANO
Podpora zpracování SNMP zpráv		ANO
Možnost úpravy zpracování událostí a alarmů včetně např. potlačení vybraných alarmů		ANO
Možnost kategorizace alarmů a událostí		ANO
Možnost nastavit zaslání upozornění na vybrané události emailem		ANO
Podpora MIB třetích stran		ANO
Možnost monitoringu parametrů definovaných v MIB třetích stran		ANO
Možnost definovat vlastní události na základě SNMP nebo SYSLOG zpráv		ANO
Možnost exportu zpráva a událostí		ANO
Možnost generovat zprávy pro nadřazený management systém		ANO

Corpus Solutions a.s.
Skládka 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IC: 15764616
DIČ: CZ23764616
Společnost Corpus Solutions a.s. je vešena v rejstřík obchodní společnosti v Praze pod spíšeovými čísly 85936

Strana 33/190

Corpus Solutions a.s.
Skládka 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IC: 15764616
DIČ: CZ23764616
Společnost Corpus Solutions a.s. je vešena v rejstřík obchodní společnosti v Praze pod spíšeovými čísly 85936

Strana 34/190

Poslání alarmů a událostí network management aplikacím třetích stran, které podporují FCAPS		ANO
Podpora API pro programatický přístup k funkcionalitě aplikace správy		ANO
Schopnost management systému nalézt automaticky zařízení v síti s využitím více různých metod pracujících s informacemi z druhé a třetí vrstvy		ANO
Schopnost management systému filtrovat nalezená zařízení - vyloučit resp. zahrnout definované adresní rozsahy		ANO
Schopnost management systému připravit konfigurační a jiné změny formou úlohy včetně schvalovacích mechanismů		ANO
Podpora pro vyhledávání informací o síťových zařízeních, připojených koncových zařízeních, uživateli, konfigurovaných parametrech, alarmech, událostech apod. napříč celým management systémem.		ANO
Správa aktivních prvků		ANO
Požadovaný počet spravovaných aktivních prvků	215	ANO
Požadavky na škálování - minimální počet spravovaných zařízení LAN / WAN sítě - aktivních prvků	25000	ANO
Požadavky na škálování - systém musí být schopen kromě LAN / WAN sítě spravovat a monitorovat také bezdrátovou síť pomocí přidáním příslušných licencí		ANO
Kompletní správa životního cyklu LAN / WAN sítě (plánování, nasazení, monitoring, troubleshooting, reporting)		ANO
Inventarizace HW síťových prvků		ANO
Inventarizace, nasazení a správa firmware aktivních prvků		ANO
Analýza vhodnosti firmware aktivních prvků pro nasazení		ANO
Generování reportů inventury aktivních prvků		ANO
Konfigurace pomocí šablon pro zefektivnění konfiguračních úloh		ANO
Inventarizace, verzování, archivace a správa konfigurací LAN / WAN sítě		ANO
Předpřipravené šablony dle doporučení výrobce - "best practice"		ANO
Možnost udržovat konfigurace v souladu s firemním standardem, identifikovat neshody		ANO
Možnost vytvářet vlastní konfigurační šablony (sekvence příkazů)		ANO
Celkové konfigurační šablony sestavené z dílčích šablon konfiguračních funkcí nebo uživatelsky definovaných konfiguračních jednotek		ANO
Podpora pro o automatizovanou konfiguraci nové připojovaných zařízení		ANO
Zobrazování alarmů a událostí z LAN / WAN sítě		ANO
Topologická mapa		ANO

Nástroje pro detekci a řešení problémů v LAN / WAN síti		ANO
Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení a jednotlivého uživatele v souladném pohledu (kontextově) pro rychlejší troubleshooting		ANO
Zobrazení informací o uživateli, koncovém či síťovém zařízení v kontextu informací souvisejících s jeho okolím a provozními parametry		ANO
Detailní monitoring LAN / WAN sítě		ANO
Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí		ANO
Monitorování výskytu koncových zařízení a uživatelů v síti		ANO
Monitoring a vyhodnocování přenosových parametrů z NetFlow		ANO
Monitoring funkcí (včetně odezvy) přenášejících aplikací		ANO
Monitoring parametrů zdraví aktivních prvků a jejich přehledné zobrazení		ANO
Možnost nastavit prahové hodnoty pro monitoring parametrů zdraví aktivních prvků		ANO
Monitoring IPv6 připojení koncových zařízení napříč pevnou i bezdrátovou sítí		ANO
Automatické dohledání portu pevné sítě s připojeným falešným access pointem		ANO
Možnost identifikovaný problém eskalovat prostředky management systému na podporu výrobce		ANO
Integrace s další aplikací pro zjišťování identity, typu, parametrů, stavu a stavu software koncových klientů pevné i bezdrátové sítě; pro monitoring bezpečnostních politik koncových klientů (ISE server)		ANO
Správa serverů a virtuálních appliance - volitelné		ANO
Možnost rozšíření o správu a monitoring připojených Cisco UCS serverů		ANO
Možnost rozšíření o správu a monitoring virtuálních strojů běžících na ESXi host (spolupráce s vCenter)		ANO
Možnost rozšíření o zpracování událostí souvisejících s výpadkem konektivity nebo chybou komponenty Cisco UCS serverů		ANO
Možnost rozšíření o schopnost detekovat výpadek Cisco UCS blade serveru, identifikovat správný blade server a graficky zobrazit vazby		ANO
Možnost rozšíření o zobrazení vazby mezi monitorovaným virtuálním strojem na ESXi hostu běžícím na Cisco UCS serveru a tímto serverem		ANO
Možnost rozšíření o sledování výkonostních parametrů monitorovaných Cisco UCS serverů		ANO
Možnost rozšíření o sledování výkonostních parametrů monitorovaných virtuálních strojů		ANO

Corpus Solutions a.s.
Skládka 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IC: 15764616
DIČ: CZ23764616
Společnost Corpus Solutions a.s. je vešena v rejstřík obchodní společnosti v Praze pod spíšeovými čísly 85936

Strana 35/190

Corpus Solutions a.s.
Skládka 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IC: 15764616
DIČ: CZ23764616
Společnost Corpus Solutions a.s. je vešena v rejstřík obchodní společnosti v Praze pod spíšeovými čísly 85936

Strana 36/190

Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimu 8x5xNBD tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému popřítavých zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevšl pochýbnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.7. Datacentrové řešení Spine-Leaf

Centralizovaná správa a konfigurace komunikační infrastruktury datového centra prostřednictvím grafického uživatelského rozhraní nebo s využitím externích nástrojů využívajících otevřená aplikační rozhraní (např. REST API). Integrovaná a centralizovaná správa jak fyzické, tak virtuální síťové infrastruktury datového centra prostřednictvím kontroléru. Definiční aplikačních politik s využitím objektově orientovaných datových modelů místo používání tradičních síťových struktur (VLAN, ACL, IP subnet...). Plně automatizovaná konfigurace komunikačních prvků a systémů datového centra na základě definovaných aplikačních politik a s využitím otevřených aplikačních rozhraní (např. OpFlex)

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Technologický celek - 1 fabrica	1 fabrica
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	AP05-81107229-1A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/data-center-virtualization

Požadovaná hodnota parametru	/application-centric-infrastructure/index.html	
	Minimální požadavky	Splněno (ANO/NE)
Formát zařízení	HW aplikace	ANO
Architektura řešení - „Spine – Leaf“		ANO
Řízení celého řešení „DC Fabric“ prostřednictvím řadiče (kontroléru)		ANO
OSPFv2		ANO
OSPFv3		ANO
IS-IS		ANO
BGPv4		ANO
BGPv6		ANO
802.1q		ANO
VXLAN enkapsulace		ANO
VXLAN bridging		ANO
VXLAN routing		ANO
Integrace fyzických i virtuálních zařízení pro L4-L7 služby		ANO
<input type="checkbox"/> Integrace s Hypervisorem VMware vSphere		ANO
<input type="checkbox"/> Integrace s Hypervisorem Microsoft Hyper-V		ANO
<input type="checkbox"/> Integrace se zařízením F5		ANO
<input type="checkbox"/> Integrace se zařízením Cisco ASA		ANO
Congestion-aware load balancing datového provozu		ANO
Podpora vytváření multi-tenant prostředí		ANO
Požadovaná funkcionální centralního řadiče (controléru)		
Řadič s redundancí pro každé datové centrum		ANO
Mód činnosti řadičů – všechny aktivní		ANO
Grafické uživatelské rozhraní součástí řešení		ANO
Přístupová práva založená na uživatelských rolích		ANO
Možnost rozdělit správu řešení mezi více vzájemně oddělených organizací (multitenantní řešení)		ANO
Dokumentované API rozhraní pro volání všech dostupných funkcí řadiče, včetně těch, které jsou použity v grafickém uživatelském rozhraní		ANO
Možnost řízení aplikačních toků prostřednictvím definice aplikačních politik, které formou logického modelu popisují požadavky aplikací na síťovou konektivitu, bezpečnost a L4-L7 služby		ANO

Corpus Solutions a.s.
Sokolova 1438/18
140 00 Praha 4
Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25794616
DIČ: CZ25794616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudů v Praze pod spisovou značkou B5936

Corpus Solutions a.s.
Sokolova 1438/18
140 00 Praha 4
Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25794616
DIČ: CZ25794616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudů v Praze pod spisovou značkou B5936

Možnost členění fyzických a virtuálních serverů do logických skupin podle své funkce a na základě charakteristik, jako je IP adresa, MAC adresa, příslušnosti do VLAN, VXLAN. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky vůči jiným skupinám.		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimu 8x5xNBD tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému popřítavých zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevšl pochýbnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.8. Spine vrstva

Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 2	2ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	N9K-C9564C	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/switches/switches/menus/g000-series-sw/switches/datasheet-c95-913726.html	
Požadovaná hodnota parametru	Minimální požadavky	Splněno (ANO/NE)
Typ přepínače	L3/L4 80G/100G	ANO

Formát zařízení	HW	ANO
Redundantní zdroj		ANO
Celková propustnost přepínače	2,88Tbps	ANO
Počet neblokovaných portů 40GE s volitelným fyzickým rozhraním typu QSFP+	36	ANO
Podpora QSFP+ rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN enkapsulace		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVFN control plane		ANO
IEEE 802.3ad		ANO
Podpora LAG, možnost konfigurace až 32 linek v rámci jednoho LAG		ANO
Počet konfigurovatelných LAGs	256	ANO
Podpora "jumbo rámec"	9216 bytů	ANO
IEEE 802.1Q		ANO
Počet aktivních VLAN	4000	ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Počet MAC záznamů	80000	ANO
Počet host IPv4 routes	200000	ANO
Počet host IPv6 routes	40000	ANO
OSPFv2		ANO
IS-IS		ANO
BGP		ANO
ECMP	64 cest	ANO
Virtualizace směrovacích tabulek (např. Virtual Routing and Forwarding (VRF))	256	ANO
OSPFv3		ANO
MP BGP		ANO
QoS – Priority Based Flow Control (IEEE 802.1Qbb)		ANO
WRED		ANO
Funkce ochrany přepínače před útoky typu odepření služby (DoS) formou vhodného omezení frekvence určitých typů rámců/paketů, které jsou zpracovávány procesorem zařízení (např. Control Plane Policing nebo ekvivalentní funkcionality)		ANO
OpenStack Neutron Plug-in		ANO
Python scripting		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO

Corpus Solutions a.s.
Sokolova 1438/18
140 00 Praha 4
Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25794616
DIČ: CZ25794616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudů v Praze pod spisovou značkou B5936

Corpus Solutions a.s.
Sokolova 1438/18
140 00 Praha 4
Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IČ: 25794616
DIČ: CZ25794616
Společnost Corpus Solutions a.s. je vedena v rejstříkového soudů v Praze pod spisovou značkou B5936

RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Syslog		ANO
Distribuovaná správa přístupů na základě rolí (Role Based Access Control)		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazez je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazez schopen sám odstranit, bylo možné v režimu 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému požadovaných zařízení přímo ze stránek výrobce na základě zaregistrovaní čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazez je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.9. Leaf vrstva – 10GB SFP+

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 4	4ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazez hlavní produktové číslo nabízeného zařízení)	C1-N9K-C93180YC-FX
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/switches/data-sheet/c93180yc-fx.html

Požadovaná hodnota parametru	Minimální požadavky	Splněno (ANO/NE)
Typ přepínače	L3/L2 přepínač	ANO
Formát zařízení	řad	ANO
Redundantní zdroj		ANO
Celková propustnost přepínače	3,6 Tbps	ANO
Počet neblokovaných portů typu 10/25GE s volitelným fyzickým rozhraním	48	ANO
Počet neblokovaných portů 40/100GE s volitelným fyzickým rozhraním typu QSFP+	6	ANO
Podpora QSFP rozhraní umožňujících přenos signálu přes duplicitní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN bridging		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)		ANO
Minimálně 32 linek jako součást Link Aggregation Group		ANO
Minimální počet konfigurovatelných Link Aggregation Groups	256	ANO
Podpora "jumbo rámců"	9216 bytes	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	32000	ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Minimální počet MAC záznamů	960000	ANO
QoS classification - ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Priority Based Flow Control (IEEE 802.1Qbb)		ANO
Approximate Fair Dropping		ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase		ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
Možnost rozšířit funkcionalitu přepínače o podporu technologie FC/FCoE NPV na SFP portech, např. formou licence		ANO
HW podpora IEEE 802.1ae (AES-GCM-XP256) na všech SFP a QSFP portech		ANO
Minimální počet host IP v4 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
OSPFv2/OSPFv3		ANO

BGP/MP-BGP		ANO
ECMP	64 směrů	ANO
IGMPv2, IGMPv3		ANO
MLDv2		ANO
IGMP snooping		ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6		ANO
PIM Bidir		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
First Hop Redundancy Protokol pro IPv6		ANO
Port ACL, VLAN ACL		ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)		ANO
Možnost rozšířit funkcionalitu přepínače o podporu line rate flow telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem), např. formou licence		ANO
Integrovaná Flow table	32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Control Plane Policing		ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače		ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů		ANO
Programovatelnost prostřednictvím rozhraní NETCONF/YANG		ANO
Streaming telemetrie pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs apod.) - iRPC/GBP transport		ANO
Streaming telemetrie - time-based a event-based triggers		ANO
Python scripting		ANO
Puppet, Chef programming		ANO
Power-on autopreprovisioning		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Počet SPAN spojení	4	ANO

Syslog		ANO
Role Based Access Control		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazez je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazez schopen sám odstranit, bylo možné v režimu 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému požadovaných zařízení přímo ze stránek výrobce na základě zaregistrovaní čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazez je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.10. Leaf vrstva 10GB – RJ45

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 2	2ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazez hlavní produktové číslo nabízeného zařízení)	C1-N9K-C93180TC-FX
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/data-sheet-c93180tc-fx.html

Požadovaná hodnota parametru	Minimální požadavky	Splněno (ANO/NE)
Typ přepínače	L3/L2 přepínač	ANO
Formát zařízení	řad	ANO

Redundantní AC zdroj (front-to-back airflow)		ANO
Celková propustnost přepínače	2,16 Tbps	ANO
Minimální počet neblokovaných portů typu 1/10GBASE-T	48	ANO
Minimální počet neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	6	ANO
Podpora 40GE rozhraní umožňujících přenos signálu přes duplicitní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)		ANO
Minimálně 32 linek jako součást Link Aggregation Group		ANO
Minimální počet konfigurovatelných Link Aggregation Groups	256	ANO
Podpora "jumbo rámců"	9216 bytes	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	3900	ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Minimální počet MAC záznamů	96000	ANO
QoS classification - ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Priority Based Flow Control (IEEE 802.1Qbb)		ANO
Approximate Fair Dropping		ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase		ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
HW podpora IEEE 802.1ae (AES-GCM-XPN-256)		ANO
Minimální počet host IPv4 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
OSPFv2/OSPFv3		ANO
BGP/MP-BGP		ANO
ECMP	64 cost	ANO
IGMPv2, IGMPv3		ANO
MLDv2		ANO
IGMP snooping		ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6		ANO
PIM BiDir		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO

First Hop Redundancy Protokol pro IPv6		ANO
Port ACL, VLAN ACL		ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)		ANO
Možnost rozšířit funkcionalitu přepínače o podporu line rate flow telemetry (schopnost monitorovat každý paket, každý datový tok procházející přepínačem), např. formou licence		ANO
Integrovaná Flow table	32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Control Plane Policing		ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače		ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů		ANO
Programovatelnost prostřednictvím rozhraní NETCONF/YANG		ANO
Streaming telemetry pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs apod.) - gRPC/GRPC transport		ANO
Streaming telemetry - time-based a event-based triggers		ANO
Python scripting		ANO
Puppet, Chef programming		ANO
Power-on autoprovisioning		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Počet SPAN spojení	4	ANO
Syslog		ANO
Role Based Access Control		ANO

Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění - tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimě 8x5x24 tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému popř. záruční služby přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropské trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevát pochopitelné zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.11. Úroveň vrstvy IGB - RJ45

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 10	10ks
Produkční číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	N9K-C9348GC-FXP
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	http://www.cisco.com/c/en/us/products/collateral/switches/nextgen-9000-series-switches/datasheet-c9348gc.html
Požadovaná hodnota parametru	Minimální požadavky (ANO/NE)
Typ přepínače	L2/L3 ANO
Formát zařízení	Plenn ANO
Redundantní AC zdroj (front-to-back airflow)	ANO
Celková propustnost přepínače	600Gbps ANO

Minimální počet portů 100/1000Base-T	48	ANO
Minimální počet neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	6	ANO
Minimální počet portů 10/25GE s volitelným fyzickým rozhraním typu SFP	4	ANO
Podpora 40GE rozhraní umožňujících přenos signálu přes duplicitní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)		ANO
Minimálně 32 linek jako součást Link Aggregation Group		ANO
Minimální počet konfigurovatelných Link Aggregation Groups	256	ANO
Podpora "jumbo rámců"	9216 bytes	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	3900	ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Minimální počet MAC záznamů	96000	ANO
QoS classification - ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Priority Based Flow Control (IEEE 802.1Qbb)		ANO
Approximate Fair Dropping		ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase		ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
Minimální počet host IPv4 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
OSPFv2/OSPFv3		ANO
BGP/MP-BGP		ANO
ECMP	64 cost	ANO
IGMPv2, IGMPv3		ANO
MLDv2		ANO
IGMP snooping		ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6		ANO
PIM BiDir		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
First Hop Redundancy Protokol pro IPv6		ANO

Port ACL, VLAN ACL.		ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 spoof(ing))		ANO
Možnost rozšířit funkcionalitu přepínače o podporu line rate flow telemetry (schopnost monitorovat každý paket, každý datový tok (rocházející/fčejinačem), např. formou licence)		ANO
Integrovaná Flow table	30000 standard	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Control Plane Policing		ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače		ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů		ANO
Programovatelnost prostřednictvím rozhraní NETCONF/YANG		ANO
Streaming telemetry pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs a...) - (RPC/GBP transport		ANO
Streaming telemetry - time-based a event-based triggers		ANO
Python scripting		ANO
Puppet, Chef programming		ANO
Power-on autoprovisioning		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Počet SPAN spojení	4	ANO
Syslog		ANO
Role Based Access Control		ANO

Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardní záručky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění - tj. uchazez je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé plátné záručky na dodaných zařízeních, kterým není Uchazez schopen sám odstranit, bylo možné v režimě 8x24x7 tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záručky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému popotávaných zařízení přímo ze stránek výrobce na základě zaregistrovaného čísla aktivovaného servisního záručního kontraktu.		ANO
--	--	-----

V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazez je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadešlá pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.12. Next-Generation Firewall

Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet kusů zařízení - úls	2ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazez hlavní produktové číslo nabízeného zařízení)	FPR120-ASA-K9	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://ccv.cisco.com/ru/en/us/support/security/firepower-4100-security-appliance/model.html	
Požadované hodnoty parametru	Minimální	Splněno (ANO/NE)
Typ zařízení	Firewall	ANO
Formát zařízení	1RU	ANO
Minimální počet 1G/10G (SFP+) Ethernet portů pro management, standardně osazených	1	ANO

Minimální počet 1G/10G (SFP+) Ethernet portů pro data, standardně osazených	8	ANO
Podporovaný počet současných otevřených spojení přes FW	15 mil.	ANO
Rychlost vytváření nových spojení přes FW	250 000/s	ANO
Propustnost firewallu	50 Gbps	ANO
Propustnost firewallu (multiprotokolový režim)	25 Gbps	ANO
Podpora L2 (transparentního) módu s podporou NAT a PAT		ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT		ANO
Podpora současně L2 a L3 v různých virtuálních FW		ANO
Podporovaný počet VLAN	30000	ANO
Redundance jednotlivých komponent v navrhované síti (fail-over bez přerušení spojení)		ANO
Podpora stateful failover - active/active i active/standby		ANO
Podpora zvyšování výkonu pomocí clusterování firewallů - složení firewallů do jednoho logického clusteru		ANO
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP		ANO
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru		ANO
Možnost sloučení až osmi fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP		ANO
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů, přikoupením licence v případě potřeby		ANO
Dynamické směrování - podpora alespoň EIGRP (RFC7868)		ANO
OSPF, BGP		ANO
Podpora IPv6 dynamického směrování - alespoň OSPFv3		ANO
Podpora Policy based Routing		ANO
Podpora samostatných směrovacích instancí na úrovni virtuálních kontextů		ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.		ANO
Podpora filtrace IPv4, IPv6		ANO
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD		ANO
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích		ANO
Stateful inspekce minimálně těchto aplikacních protokolů: HTTP, FTP, Instant Messenger, File Sharing, SIP, H.323, SCCP, SMTP, ESMP/T, DNS, RPC, CIFS, MSRPC, NETBIOS		ANO

Možnost filtrace komunikace Botnet sítě s využitím databázi o důvěryhodnosti adres v Internetu		ANO
Podpora NAT64 a DNS64		ANO
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.		ANO
Možnost rozšíření o funkce NextGen FW		ANO
Možnost rozšíření o funkce NextGen IPS		ANO
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele		ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy		ANO
Možnost zařazení do SDN řešení - kontrolerem řízená infrastruktura (APIC)		ANO
Možnost správy fw pravidel přes příkazový řádek z lokální konzole a vzdáleným přístupem protokolem ssh		ANO
Vzdálená správa konfigurace přes grafické rozhraní bez nutnosti instalace tušého klienta+A26		ANO
Při použití clusteru se spravuje pouze jeden logický prvek		ANO
Distribuce a správa SW firewallu, dalších modulů (např. pro VPN), konfiguraci, licencí z grafického rozhraní managementu		ANO
Zobrazení logů a událostí v grafickém rozhraní správy s mapováním na konfiguraci bezpečnostních politik		ANO
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování		ANO
Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap		ANO
Výkon a funkcionalita VPN (požadováno)		
Propustnost VPN koncentrátora (šifrovaní 3DES/AES)	10Gbps	ANO
Počet současných šifrovaných spojení	10000	ANO
Podpora IPsec VPN		ANO
IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol		ANO
Podpora nového protokolu pro výměny klíčů IKEv2		ANO
Podpora šifrovacích metod - minimálně: DES, 3DES, AES-128, AES-192, AES-256		ANO
Podpora kontrolních mechanismů: MD5, SHA		ANO
Podpora NextGen šifrovacích algoritmy: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256		ANO

Podpora komponenty Suite-B: SHA-2 mechanismus s metodami: SHA-256, SHA-384	ANO
Podpora šifrovacích algoritmů eliptických křivek (součást Suite-B): ECDH, ECDSA	ANO
Podpora SSL VPN	ANO
Jednotný klient pro IPsec (IKEv2) i SSL VPN	ANO
SSL VPN klient k dispozici pro všechny běžné desktopové OS: XP SP2+ 32-bit(a86) a 64-bit(x64), Vista (32-bit a 64-bit), Windows 7 (32-bit a 64-bit), MAC OS X(10.5, 10.6.x, 10.7.x, 10.8.x), Linux	ANO
VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)	ANO
VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů	ANO
SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS	ANO
Podpora TLS i DTLS pro SSL připojení	ANO
Podpora SSL VPN v tunelovém režimu s distribucí VPN klientského SW přímo z FW	ANO
Podpora současné autentizace koncové stanice i uživatele	ANO
Podpora definice pravidel pro VPN přístup přímo prostředky FW	ANO
Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phonu a tabletů	ANO
Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)	ANO
Podpora definice různých LDAP nebo AD serverů podle mapování uživatelů na skupiny s využitím RADIUS, LDAP nebo hodnot v certifikátu	ANO
Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačních systémů	ANO
Podpora autentizačních mechanismů: lokální databáze na FW, RADIUS, Windows NT LAN Manager (NTLM), Active Directory Kerberos, RSA softID, RSA securID, Lightweight Directory Access Protocol (LDAP), digitální certifikáty (X.509), smartcards	ANO
Podpora veřejných CA, včetně možnosti CA přímo na firewallu	ANO
Možnost současné autentizace AAA a certifikátem	ANO
Možnost mapování některého DN pole certifikátu na uživatelskou identitu	ANO
Podpora CRL a OCSP pro kontrolu revokace certifikátů	ANO
Podpora čistého IPv6 přístupu na VPN koncentrátor	ANO

Funkce IPS (v případě rozšíření)		
Propustnost aplikačního FW (next-gen FW) – (top parametry)	20Gbps	ANO
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	15Gbps	ANO
Propustnost aplikačního FW nebo IPS (next-gen FW, IPS) (transakční profil, 440B HTTP průměrná velikost paketu)	8Gbps	ANO
Možnost definovat typ provozu předávaný k inspekci do IPS	ANO	
Podpora také IDS režimů – pasivního monitorování (TAP režim)	ANO	
Možnost definovat bypass provozu při zahájení nebo nedostupnosti IPS funkce	ANO	
Možnost obejít IPS funkci při zahájení nebo nedostupnosti	ANO	
Podpora 802.1Q tagovaných rámců	ANO	
Inspekce pro IPv4 i IPv6	ANO	
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	ANO	
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	ANO	
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelnosti a databáze systémů na internetu s poškozenou reputací	ANO	
Podpora aplikace pro psaní zákaznických filtrů	ANO	
Podpora importu komunitních filtrů/signatur Snort	ANO	
IPS musí umět detekovat a blokovat útoky přízkumných aktivit	ANO	
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	ANO	
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	ANO	
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Děle musí poskytovat i ochranu pro protokoly využívané v IP telefonii	ANO	
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	ANO	
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	ANO	
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	ANO	

Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	ANO
Možnost definice uživatelské vrstvy politik	ANO
Předefinování pravidel přes vrstvy IPS politik – platí relevantní pravidla v nejvyšší vrstvě IPS politik	ANO
Různé politiky lze sdílet a aplikovat na různé senzory	ANO
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávisle na aktuálních databázích AV dodavatelů	ANO
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	ANO
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	ANO
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	ANO
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spuštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	ANO
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	ANO
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	ANO
IPS musí být plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	ANO
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	ANO
Možnost automatické i manuální klasifikace stanice jako „kritické“ se zohledněním v pravidlech, reportech apod.	ANO
Podpora „remediation“ modulu pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	ANO
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	ANO
Podpora databází reputací adres v Internetu (Security Intelligence)	ANO
Funkce Next-Gen FW (v případě rozšíření)	
Možnost definovat typ provozu předávaný k inspekci do Next-Gen FW	ANO
Podpora pasivního monitorování (TAP režim)	ANO

Možnost by-pass provozu Next-Gen FW funkce při zahájení nebo nedostupnosti	ANO
Podpora 802.1Q tagovaných rámců	ANO
Podporovaných aplikací, min. 3000	ANO
Kategorie aplikací (nebezpečné, důležité, apod.)	ANO
URL kategorií	ANO
Kategorizovaných světových URL, min. 280 milionů	ANO
Řízení přístupu k WWW - Web Usage Control (WCU)	ANO
Filtrace podle typů aplikací webových i ne-webových	ANO
Filtrace podle reputace serverů	ANO
SSL inspekce (dekrypce/enkrypce)	ANO
Security Intelligence database – známé uzly botnet sítě C&C	ANO
Security Intelligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	ANO
Možnost integrovat vlastní reputační databáze	ANO
Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)	ANO
Filtry mohou zohlednit roli a identitu uživatele	ANO
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	ANO
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě (Network Behavior Analysis - NBA)	ANO
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	ANO
<input type="checkbox"/> Operační systém Dodavatel OS	
<input type="checkbox"/> Použití síť. protokoly Použití síť. služby	
<input type="checkbox"/> Otevřené porty síť. služeb	
<input type="checkbox"/> Potenciální zranitelnosti	
Přehled o síťových spojení má poskytovat minimálně tyto informace:	ANO
<input type="checkbox"/> Čas startu a konce flow Akce (allow, deny,...)	
<input type="checkbox"/> Důvod případného blokování	
<input type="checkbox"/> Zdrojová a cílová adresa Vstupní a výstupní zóna	
Vstupní a výstupní rozhraní Zdrojový a cílový port	
<input type="checkbox"/> Aplikační protokol	
<input type="checkbox"/> IPS událost, pokud vznikne Riziková úroveň IPS	
údálosti Použití síťová aplikace Rizikovitost aplikace	
<input type="checkbox"/> „Business impact“ aplikace	
<input type="checkbox"/> Množství přenesených dat	
Správa Next-Gen FW a IPS (v případě rozšíření)	
Možnost centrální správy při nasazení více firewallů	ANO

Při centrální správě: možnost sdílených bezpečnostních politik	ANO
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního systému (centrální dohledové konzole)	ANO
Centrální dohledové konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdravotí boxů, apod.	ANO
Centrální dohledové konzole musí být schopna posílytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	ANO
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	ANO
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typu incidentů, aplikací, koncových stanic	ANO
Centrální dohledové konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	ANO
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	ANO
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	ANO
Centrální dohledové konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	ANO
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailů, lokální události, apod.	ANO
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	ANO
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM: <input type="checkbox"/> ArcSight <input type="checkbox"/> BMC Remedy Trustwave NetForensics Novell <input type="checkbox"/> Hawk Network Defense QILabs-QRadar <input type="checkbox"/> Log Rhythm SIEM 2.0 LogLogic <input type="checkbox"/> Splunk	ANO
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	ANO
Podpora JDBC API pro přístup v externích systémech k databázím centralizovaného managementu	ANO
Podpora řízeného přístupu podle rolí administrátorů	ANO
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	ANO

Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	ANO
Workflow pro předávání „ticketů“ mezi administrátory	ANO
Konkrétní bezpečnostní incident až na úrovni balíku lze přiložit k danému „ticketu“ pro další analýzu	ANO
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	ANO
Zákaznický definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	ANO
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardní záruky za jakost běžné užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterým není Uchazeč schopen sám odstranit, bylo možné v režimu 8x5x24 tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému popotávaných zařízení přímo ze stránek výrobce na základě registrovaní čísla aktivovaného servisního záručního kontraktu.	ANO
V databázi výrobce musí být Zadavatel uveden jako první uživatel zboží. Zadavatel požaduje originální a nové zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel i či dodání zařízení požádá.	ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochopitelné zřejmé, že výrobce tohoto řešení má implementován tzv. „SDL - secure development lifecycle“ při vývoji svých produktů a tzv. „SIRT - Security Incident Response Team“ pro reportování bezpečnostních incidentů spojených s nabízenými produkty.	ANO

Ve spojení s centralizovaným managementem tyto bezpečnostní služby zajišťují funkce „Next-Generation“ FW (dále jenom NGFW) a IPS a disponují tak možnostmi detekce a potlačení pokročilých a cílených typů útoků. Tyto, a další, mechanismy jsou explicitně vyžadované ve specifických vyhláškách zákona 183/2014 Sb. o kybernetické bezpečnosti:

- §17 Nástroj pro ochranu integrity komunikačních sítí
- §20 Nástroj pro ochranu před škodlivým kódem

- §22 Nástroj pro detekci kybernetických bezpečnostních událostí
- §23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- §24 Aplikace bezpečnosti
- §26 Nástroje pro zajištění vysoké úrovně dostupnosti

Ve spojení s používaným a plánovaným řešením pro centralizované řízení a monitorování přístupu do sítě (LAN, WiFi, VPN) podle kontextu (detailní znalost o uživateli a přístupové platformě) lze reagovat i na požadavky:

- §18 Nástroj pro ověřování identity uživatelů
- §19 Nástroj pro řízení přístupových oprávnění

Klíčové nové vlastnosti takto rozšířených NGFW jsou:

- IPS nebo IDS detekční a ochranný systém se schopností automatického ladění souboru IPS/IDS signatur podle sledování prostředí a automatickým vyhodnocením stupně nebezpečnosti útoků v relevanci s metodou útoku a zranitelností cílového systému
- Automatické potlačení útoku (Remediation) na základě korelace událostí s nastavenými pravidly pro odpovídající typy reakce (např. signalizace požadavku směrem do jiných síťových zařízení pro odpojení stanice, nastavení přístupového filtru, přesměrování apod.)
- Interní korelace událostí (typ útoku, komunikace v botnet síti, přenos malware, apod.) pro automatickou detekci kompromitovaných stanic
- Kontinuální analýza síťového prostředí s automatickou reakcí na porušení pravidel (compliance) – např. detekce nepovoleného OS v určitém segmentu sítě, vyhoštění ze „standardního“ obrazu komunikace apod.
- Detekce přenosu malware, včetně zero-day typů souborů, s možností retrospektivního monitorování (trajektorie přenosu souborů sítí: první stanice která soubor získala, protokoly a metody přenosu v rámci sítě, reakce senzorů nebo agentů na koncových stanicích na daný malware, apod.)
- Aplikace firewall s možností definice vlastních aplikací (podpora OpenAppID aplikací signatur)
- URL filtrace podle web kategorií, reputace, konkrétních URL
- Integrované Security Intelligence blacklistů – DNS, URL, známé adresy botnet sítě, problematické stroje v Internet
- Antimalware ochrana – analýza přenášených souborů s možností dynamické analýzy a sandboxing se záznamem přenosu všech souborů sítí pro následnou retrospektivní analýzu

Služby NGFW a její komponenty se spravují na fyzickém nebo virtualizovaném zařízení. Pro kompletní komunikaci administrátorů s centralizovaným

managementem (analýza komunikace, bezpečnostních událostí, kontextová viditelnost, atd.) je k dispozici plně webové GUI. Není potřeba žádný klientský SW.

- Veškeré dashboardy lze modifikovat
- Na základě korelace bezpečnostních incidentů jsou pro všechny stanice v síti poskytovány tzv. indikátory kompromitace (IoC)
- NGFW disponuje funkcí učení se prostředí pomocí strojového učení (machine learning) a korelace se znalostmi databáze (dodavatele) poskytují rychlý a názorný pohled na trendy, typy komunikací, stanic, událostí atd. v síti.
- Provoz, který je řádkem pravidla firewallu explicitně propuštěn může být dále kontrolován detekčními systémy IPS/IDS, systém umožňuje dále analyzovat přenášené soubory pomocí služby pokročilé ochrany před malwarem, sledovat zdraví, monitorovat prostředí, atd.
- NGFW API dovoluje integraci se systémy SIEM, log servery apod.
- Centralizovaný management integruje i reportovací systém. K dispozici jsou hotové šablony, přičemž lze definovat i vlastní obsah reportů (grafické dashboardy, tabulky, grafy apod.)

2.13. Virtuální privátní síť, vzdálené přístupy do sítě

Suplikant, který centralizuje, sjednocuje a zabezpečuje kontrolu přístupu do sítě na základě bezpečnostních politik pro koncové uživatele připojené přes kabelové, bezdrátové sítě nebo VPN. Poskytuje rozsáhlou viditelnost a přesnou identifikaci pomocí profilování koncových zařízení čím přispívá k snížení počtu neznámých koncových bodů v síti. Zjednodušuje možnost připojení pro hosty do Guest sítě a jejich správu prostřednictvím plně přizpůsobitelných mobilních nebo desktop portálů. Urychluje BYOD a Enterprise Mobility se snadným „out-of-the-box“ nastavením a správu certifikátů pro interní zařízení, všechno s jednotným a přehledným managementem. Umožňuje automaticky reagovat na bezpečnostní hrozby prostřednictvím integrace s NGFW, kde řešení pro kontrolu přístupu do sítě na základě sdílených informací může infikované koncové zařízení pozorovat, omezit mu přístup, nebo napomoci v remediálním procesu.

□ Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 5300	8300ks (lic)
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	L-AC-PLS-LIC L-AC-APX-LIC
Odkaz na www stránku výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém	https://www.cisco.com/c/en/us/products/docs/secure/5300/5300-lic.html

žájeze	/security/anyconnect-secure-mobility-client/index.html	Minimální požadavky	Splněno (ANO/NE)
Požadovaná hodnota parametru			
Podpora SSL VPN i IPsec VPN			ANO
IPsec VPN s podporou databáze: RFC 2408 – Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 – The Internet Key Exchange (IKE), RFC 2412 – OAKLEY Key Determination Protocol			ANO
Podpora nového protokolu pro výměny klíčů IKEv2			ANO
Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256			ANO
Podpora komponenty Šuite-B: SHA-2 mechanismu s metodami: SHA-256, SHA-384			ANO
Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA			ANO
Jednotný klient pro IPsec (IKEv2) i SSL VPN			ANO
SSL VPN klient k dispozici pro všechny běžné desktopové OS: XP SP2+ 32-bit(x86) a 64-bit(x64), Vista (32-bit a 64-bit), Windows 7 (32-bit a 64-bit), MAC OS X(10.5, 10.6.x, 10.7.x, 10.8.x), Linux			ANO
Distribuce VPN klient SW může poskytnout i jednotný 802.1X supplicant s autentizačními metodami: EAP-TLS, tunelovaný EAP-TLS, EAP-MSCHAPv2 nebo EAP-GTC, chráněný pomocí EAP-PEAP, EAP-FAST nebo EAP-TTLS			ANO
VPN klient může být distribuován s 802.1X ataba řešiči i efektivní machine/user autentizací podle EAP-FAST (EAP Chainina)			ANO
VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů			ANO
SSL VPN klient je k dispozici pro ataba mobilní atabase na bázi Android a Apple iOS.			ANO
Podpora TLS i DTLS pro SSL připojení			ANO
Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. V AD)			ANO
Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu atabase a operačního systému			ANO
Podpora clientless SSL VPN přístupu s pluginy pro aplikace (např. SSH, RDP, VNC), zpřístupnění interních webových aplikací, souborů sdílených přes CIFS, přístup na aplikace pomocí port forwarding nebo pomocí tenkého klienta na úrovni aplikace			ANO

Podpora autentizačních mechanismů: lokální atabase na FW, RADIUS, Windows NT LAN Manager (NTLM), Active Directory Kerberos, RSA softID, RSA securlD, Lightweight Directory Access Protocol (LDAP), digitální certifikáty (X.509), smartcards			ANO
Podpora veřejných CA, včetně možnosti CA přímo na firewallu			ANO
Možnost současné autentizace AAA a certifikátem			ANO
Podpora CRL a OCSP pro kontrolu revokace certifikátů			ANO
Podpora SSO metod: KCD, Netegrity, ClearTrust, SAML, NTLM/FTP/CIFS pass-through, HTTP pass-through pomocí formuláře; HTTP-POST pomocí substituci proměnných			ANO
Podpora IPv6 adresních rozsahů a přiřazení IPv6 adres klientům v případě dual-stack přístupu přes IPv4 infrastrukturu			ANO
Podpora čistého IPv6 přístupu na VPN koncentrátor			ANO
Možnost jednotné správy přístupu uživatelů přes VPN ale i lokálně na LAN a WIFI			ANO
Klient musí umožňovat instalaci jednotlivých svých modulů, které dovoří integraci a viditelnost pro uživatele následujících bezpečnostních řešení poptávaných v jiných částech:			ANO
body			
<input type="checkbox"/> Pokročilá ochrana proti malware pro koncové			
<input type="checkbox"/> Řízení přístupu k síťovým prostředkům			ANO
<input type="checkbox"/> Ochrana emailové komunikace			
<input type="checkbox"/> Ochrana webových komunikace prostřednictvím			ANO
webové brány			
<input type="checkbox"/> Ochrana webových komunikace prostřednictvím			
DNS			
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardní záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řídným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimě 8x5xNBD tuto záradu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.			ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při doání zařízení požádá.			ANO

Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevši pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.			ANO
--	--	--	-----

2.14. Přístupové přepínače s 24 PoE porty

LAN L3 přepínač s 24x 1Gb/s POE porty a 8x 10Gb/s SFP+ porty. Slouží jako přístupový přepínač pro připojení zařízení jako jsou uživatelská PC a tiskárny. Je to nejdílná součást řady skupiny a virtualizované platformy nad sítí, kdy veškerý provoz na něm bude plně směrovan pomocí VxLAN enkapsulace. Přepínač podporuje plnohodnotnou integraci služby s rozpoznávaní identity, které umožňuje dělit uživatele do definovaných skupin a definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu, která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

<input type="checkbox"/> Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 80	80ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C9300-24P-A	
Odkaz na www stránku výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/support/switches/catalogs/c9300-24p-a-switch/model.html	
Požadovaná hodnota parametru	Minimální požadavky	Splněno (ANO/NE)
Typ přepínače	L3/L2 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Sdílení výkonu napájecích zdrojů napříč celým stohem		ANO
Stateful Switch Over v rámci stohu		ANO
Non-stop Forwarding		ANO
Možnost instalovat interní redundantní napájecí zdroj		ANO
Interní redundantní napájecí zdroj požadován		ANO
Datový stohovací kabel požadován		ANO

Napájecí stohovací kabel požadován			ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48		ANO
Minimální PoE budget	430W		ANO
Uplink porty	8x10GE SFP+		ANO
Min. velikost sdíleného systémového bufferu	16MB		ANO
Velikost MAC address tabulky	30000		ANO
Min. počet IPv4 routes	32000		ANO
Min. počet IPv6 routes	16000		ANO
Min. počet konfigurovatelných security ACL	5000		ANO
IEEE 802.3ad (Link Aggregation)			ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis			ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku			ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	128		ANO
IEEE 802.1Q			ANO
Minimální počet aktivních VLAN	4000		ANO
IEEE 802.1x			ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)			ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)			ANO
Možnost provozu 802.1x v tzv. audit módu bez omezení přístupu koncových uživatelů			ANO
RADIUS CoA			ANO
Podpora instance spanning-tree protokolu per VLAN			ANO
IEEE 802.1w - Rapid Spanning Tree Protocol			ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí			ANO
Podpora jumbo rámců (min. 9198 bytes)			ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)			ANO
Směrování protokolů IPv4 a IPv6 v hardware			ANO
OSPFv2			ANO
OSPFv3			ANO
ISIS			ANO
BGPv4			ANO
Graceful Insertion and Removal			ANO
IP Multicast (PIM SSM, PIM SM)			ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)			ANO
MPLS VPN			ANO
MPLS VPN - 6VPE			ANO

First Hop Redundancy Protocol (např. VRRP, HSRP)		ANO
Reverse path check (uRPF) pro IPv4 i IPv6		ANO
IGMPv2, IGMPv3		ANO
IGMP snooping		ANO
MLD snooping		ANO
DHCP relay		ANO
Minimální počet HW QoS front	1	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Strict Priority Queue		ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 6m n 8	ANO
First Hop Redundancy Protocol pro IPv6 (HSRP nebo VRRP)		ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)		ANO
IPv6 QoS		ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)		ANO
IPv6 Port ACL, VLAN ACL		ANO
Možnost definovat povolené MAC adresy na portu		ANO
PACL, VACL		ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy		ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru		ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP		ANO
Ochrana proti nahrání modifikovaného softwaru do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autenticitu a integritu jak bootloadru, tak i samotného operačního systému zařízení prostřednictvím interních HW (prostředků - tzv. trusteč) modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IEEE 802.3af		ANO
IEEE 802.3at		ANO
IEEE 802.3az		ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu		ANO
Multicast DNS (mDNS) gateway		ANO

Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenesených aplikací (DPI na 7. vrstvě OSI modelu dle aplikacních signatur)		ANO
Application Visibility - Monitorování aplikacních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvencí čísla, hodnota TTL, ICMP kód, IGMP type		ANO
Application Visibility - Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS		ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
CLI rozhraní		ANO
Analýza šifrovaného datového provozu		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmwaru		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Podpora network boot (PXE) přes IPv4 i IPv6		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		ANO

Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardní záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobci zařízení tak, aby v případě závady v průběhu celé pětiléte záruky na dodaných zařízeních, kterou není uchazeč schopen sám odstranit, bylo možné v režimě 8x24x7 tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětiléte záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému používaných zařízení přímo ze stránek výrobce na základě zaregistrovaní čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochopitelné zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.15. Distribuční přepínače

LAN L3 přepínač s 48x 1Gb/s POE porty a 8x 10Gb/s SFP+ porty. Prvek je v roli hraničního přepínače, který slouží jako lokální podřízený síťový kontroler zajišťující konektivitu do WAN a management řízených skupin a virtualizované platformy nad sítí. Přepínač podporuje plnohodnotnou integraci služby na rozpoznávání identity, které umožňuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu, která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 73	73ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uveďte Uchazeč hlavní produktové číslo nabízeného zařízení)	C9300-48P-A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v češtině nebo anglickém	https://www.cisco.com/c/en/us/products/c9300-series-switches/specifications.html

Požadovaná hodnota parametru	Minimální požadavky	Společno (ANO/NE)
Typ přepínače	L3/L5 ethernet	ANO
Formát přepínače	stohovací	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Sdílení výkonu napájecích zdrojů napříč celým stohem		ANO
Stateful Switch Over v rámci stohu		ANO
Non-stop Forwarding		ANO
Možnost instalovat interní redundantní napájecí zdroj		ANO
Interní redundantní napájecí zdroj požadován		ANO
Datový stohovací kabel požadován		ANO
Napájecí stohovací kabel požadován		ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	ANO
Počet portů 1/2.5/5/10 Gbase-T s PoE napájením		ANO
Minimální PoE budget	430W	ANO
Uplink porty	8x10GE SFP+	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	30000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
IEEE 802.3ad (Link Aggregation)		ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis		ANO
Minimálně 8 linek jako součást Link Aggregation Group tranku		ANO
Minimální počet konfigurovatelných Link Aggregation Group tranků	128	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	3000	ANO
IEEE 802.1x		ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresu, Web autentizaci)		ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)		ANO
Možnost provozu 802.1x v tzv. audit módu bez omezení přístupu u koncových uživatelů		ANO

RADIUS CoA		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Směrování protokolů IPv4 a IPv6 v hardware		ANO
OSPFv2		ANO
OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
MPLS VPN		ANO
MPLS VPN - 6VPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
Reverse path check (rPF) pro IPv4 i IPv6		ANO
IGMPv2, IGMPv3		ANO
IGMP snooping		ANO
MLD snooping		ANO
DHCP relay		ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking – DSCP, CoS		ANO
QoS - Strict Priority Queue		ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 000/100	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)		ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)		ANO
IPv6 QoS		ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)		ANO
IPv6 Port ACL, VLAN ACL		ANO
Možnost definovat povolené MAC adresy na portu		ANO
PACL, VACL		ANO

Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy		ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru		ANO
Bezpečnostní funkce umožňující inspekci provozu protokolů ARP		ANO
Ochrana proti nahrazení modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IEEE 802.3az		ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu		ANO
Multicast DNS (mDNS) gateway		ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenesených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/clová MAC adresa, zdrojová/clová IP adresa, zdrojová/clová VLAN, TCP flags, TCP sekvencovní číslo, hodnota TTL, ICMP kód, IGMP typ		ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS		ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
CLI rozhraní		ANO
Analýza šifrovaného datového provozu		ANO
Analýza šifrovaného datového provozu		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní události v systému zařízení		ANO
Application hosting		ANO

Corpus Solutions a.s.
Sokolova 1638/II
140 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IC: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vědecká a výzkumná společnost v Praze pod spisovou značkou B3936

Strana 89/190

Corpus Solutions a.s.
Sokolova 1638/II
140 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IC: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vědecká a výzkumná společnost v Praze pod spisovou značkou B3936

Strana 90/190

Aplikace softwarových záplat, nikoli povyšování celého firmware		ANO
Streaming telemetry prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Podpora network boot (iPXE) přes IPv4 i IPv6		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardní záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závdav v průběhu celé pětileté záruky na dodaných zařízeních, kterým není Uchazeč schopen sám odstranit, bylo možné v režimu 8x5xNBD tuto závdavu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nově verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit povolení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doložení výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochopnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.16. Přístupové přepínače s 48 PoE porty

LAN L3 přepínač s 48x 1Gb/s POE porty a 8x 10Gb/s SFP+ porty. Slouží jako přístupový přepínač pro připojení zařízení jako jsou uživatelská PC a tiskárny. Je to nedílná součást řízené skupiny a virtualizované platformy nad sítí, kdy veškerý provoz na něm bude plně směrován pomocí VxLAN enkapsulace. Přepínač podporuje plnohodnotnou integraci služeb na rozpozdnání identity, které umožňuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu,

která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

Základní údaje		Nabízená hodnota
Výrobce zařízení		CISCO
Počet kusů zařízení - 72		72
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uveďte Uchazeč hlavní produktové číslo nabízeného zařízení)		C9300-48P-A
Odkaz na www stránku výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v češtině nebo anglickém jazyce		https://www.cisco.com/c/en/us/support/software/catalyst9300-48p-a-switch/model.html
Požadovaná hodnota parametru	Minimální požadavky	Společné (ANO/NE)
Typ přepínače	L3/L4 přepínač	ANO
Formát přepínače	Stohovatelý	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Sdílení výkonu napájecích zdrojů napříč celým stohem		ANO
Stateful Switch Over v rámci stohu		ANO
Non-stop Forwarding		ANO
Možnost instalovat interní redundantní napájecí zdroj		ANO
Interní redundantní napájecí zdroj požadován		ANO
Datový stohovací kabel požadován		ANO
Napájecí stohovací kabel požadován		ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	ANO
Minimální PoE budget	430W	ANO
Uplink porty	8x10GE SFP+	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	3000	ANO
IEEE 802.3ad (Link Aggregation)		ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis		ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku		ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	228	ANO

Corpus Solutions a.s.
Sokolova 1638/II
140 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IC: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vědecká a výzkumná společnost v Praze pod spisovou značkou B3936

Strana 91/190

Corpus Solutions a.s.
Sokolova 1638/II
140 00 Praha 4
Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz
IC: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vědecká a výzkumná společnost v Praze pod spisovou značkou B3936

Strana 92/190

IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	10000	ANO
IEEE 802.1x		ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)		ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)		ANO
Možnost provozu 802.1x v tzv. audit módu bez omezení přístupu koncových uživatelů		ANO
RADIUS CoA		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Směrování protokolů IPv4 a IPv6 v hardware		ANO
OSPFv2		ANO
OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
MPLS VPN		ANO
MPLS VPN - 6VPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
Reverse path check (uRPF) pro IPv4 i IPv6		ANO
IGMPv2, IGMPv3		ANO
IGMP snooping		ANO
MLD snooping		ANO
DHCP relay		ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Strict Priority Queue		ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO

QoS-Hierarchical QoS	2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)		ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)		ANO
IPv6 QoS		ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)		ANO
IPv6 Port ACL, VLAN ACL		ANO
Možnost definovat povolené MAC adresy na portu		ANO
PACL, VAACL		ANO
IEEE 802.1ae na uplink portech		ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech		ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy		ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru		ANO
Bezpečnostní funkce umožňující inspekci provozu protokolů ARP		ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloadeu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IEEE 802.3af		ANO
IEEE 802.3at		ANO
IEEE 802.3az		ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu		ANO
Multicast DNS (mDNS) gateway		ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenesených aplikací (DPI na 7. vrstvě OSI modelu dle aplikacních signatur)		ANO
Application Visibility - Monitorování aplikacních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvencovní čísla, hodnota TTL, ICMP kód, IGMP type		ANO
Application Visibility - Schopnost detekce bezpečnostních hrozeb v šířovaném provozu, např. v HTTPS		ANO

Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
CLI rozhraní		ANO
Analýza šířovaného datového provozu		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní události v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmwaru		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Podpora network boot (PXE) přes IPv4 i IPv6		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o poskytnutí a výrobci zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimě 8x24x7 tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO

Součástí nabídky musí být doložit výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.

2.17. Centrální přepínače

LAN L3 přepínač s 4x 10Gb/s SFP+ porty. Slouží jako centrální přepínač pro připojení přístupových a distribučních přepínačů v rámci řízené skupiny a virtualizované platformy sítě, kde veškerý provoz na něm bude plně směrován pomocí VXLAN enkapsulace. Přepínač podporuje plnohodnotnou integraci služby na rozpoznávání identity, která umožňuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šířovaného provozu, která umožňuje zachytávat závažný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 6	6ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C9500-48X-A
Odkaz na www stránku výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/data_sheet_C95-21878.html
Požadovaná hodnota parametru	Minimální požadavky (ANO/NE)
Typ přepínače	L3/L2 přepínač ANO
Minimální počet neblokovaných portů 1/10GE s voltelným fyzickým rozhraním typu SFP+	40 ANO
Uplink porty	8x10GE SFP+ ANO
Interní redundantní napájecí zdroj	ANO
Min. velikost sdíleného systémového bufferu	64MB ANO
Velikost MAC address tabulky	64000 ANO
Min. počet IPv4 routes	64000 ANO
Min. počet IPv6 routes	32000 ANO
Min. počet konfigurovatelných security ACL	18000 ANO
Flexibilní alokace SRAM a TCAM zdrojů	ANO

IEEE 802.3ad (Link Aggregation - LAG)		ANO
Minimální počet aktivních VLAN	4000	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
OSPFv2, OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	10	ANO
MPLS VPN		ANO
MPLS VPN - GVPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6		ANO
Reverse path check (uRPF)		ANO
Minimální počet HW QoS front	8	ANO
QoS - Strict Priority Queue		ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 úrovně	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard)		ANO
Port ACL, VLAN ACL		ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloadera, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IPv6 Port ACL, VLAN ACL		ANO
IEEE 802.1AR na všech portech		ANO
Source-Group Tag Exchange Protocol nebo ekvivalentní		ANO
IGMPv2/v3 snooping		ANO

Corpus Solutions a.s. Štikovská 1838/18 140 00 Praha 4
Tel: +420 241 020 333 E-mail: sales@corpus.cz Internet: www.corpus.cz
IČ: 25744616 DIČ: CZ25744616 Společnost Corpus Solutions a.s. je vedena u rejčířského soudu v Praze pod spisovou značkou B5936 Strana 97/190

MLD snooping		ANO
Multicast DNS (mDNS) gateway		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenesených aplikací (DPI na 7. vrstvě OSI modelu dle aplikacních signatur)		ANO
Application Visibility - Monitorování aplikacních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP v3		ANO
Export monitorovaných dat ve formátu NetFlow v3 nebo IPFIX SSHv2		ANO
Analýza šifrovaného datového provozu		ANO
CLI rozhraní		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmwaru		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardní záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění - tj. uchazez je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé péřené záruky na dodaných zařizeních, kterou nelze Uchazez schopen sám odstranit, bylo možné v režimě 8x5xNBD tuto záadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky ležárně stahovat nové verze softwaru a ovladačů		ANO

Corpus Solutions a.s. Štikovská 1838/18 140 00 Praha 4
Tel: +420 241 020 333 E-mail: sales@corpus.cz Internet: www.corpus.cz
IČ: 25744616 DIČ: CZ25744616 Společnost Corpus Solutions a.s. je vedena u rejčířského soudu v Praze pod spisovou značkou B5936 Strana 98/190

systemu poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazez je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevít pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.18. Agregacní směrovač

Modulární agregacní směrovač s vysokou propustností, který umožňuje bezpečné a šifrované připojení do WAN sítí. Prvek bude instalován jako součást virtualizované sítě, kde bude sloužit jako koncentrátor zabezpečené šifrované komunikace mezi centrálním kontrolérem a hraničními prvky v jednotlivých řízených skupinách a virtualizovaných sítích.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 2	2ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazez hlavní produktové číslo nabízeného zařízení)	C1-ASR1001-X/K9
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/support/routers/asr-1001-x-router/model.html
Požadovaná hodnota parametru	Minimální požadavky (ANO/NE)
Typ zařízení	Směrovač
Formát zařízení	Modulární ANO

Minimální počet osaditelných slotů moduly rozhraní v šasi	2	ANO
Povyšitelnost o 2x 10GE SFP+ bez výměny HW		ANO
Požadovaný počet portů GigabitEthernet	6x SFP+	ANO
Redundantní AC napájecí zdroj (interní)		ANO
Oddělený procesor pro funkce směrování a forwardování paketů		ANO
Směrování IPv4		ANO
Směrování IPv6		ANO
Propustnost systému	2,9Tb/s	ANO
Kapacita povyšována licenčně, bez povyšování HW		ANO
Maximální dosažitelná kapacita bez povyšování HW	50 Gbps	ANO
Paketový výkon směrovače	15Mpps	ANO
Softwarová redundance routovacího procesu	povyšitelná licenčně	ANO
Funkce stavového firewallu		ANO
Stavová redundance firewallu/NAT i mezi šasi	povyšitelná licenčně	ANO
Zabezpečení přenosu metodou IPsec		ANO
Funkce klasifikace aplikací, měření jejich odezvy a následná aplikace příslušných přenosových politik	povyšitelná licenčně	ANO
Nástroj správy klasifikace aplikací (ev. licence pro zařízení)	povyšitelná licenčně	ANO
Funkce NAT mezi IPv6 a IPv4	povyšitelná licenčně	ANO
Minimální počet záznamů ve směrovací tabulce - IPv4	1M	ANO
Minimální počet záznamů ve směrovací tabulce - IPv6	0,5M	ANO
IEEE 802.3ad		ANO
OSPFv2		ANO
BGPv4		ANO
Podpora 4 byte AS numbers in BGP		ANO
Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
GRE (Generic Routing Encapsulation)		ANO
Policy-based routing podle ACL		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
IGMPv2, IGMPv3		ANO
uRPF		ANO
DHCP relay		ANO
First Hop Redundancy Protokol pro IPv6		ANO
OSPFv3		ANO
MP BGP		ANO

Corpus Solutions a.s. Štikovská 1838/18 140 00 Praha 4
Tel: +420 241 020 333 E-mail: sales@corpus.cz Internet: www.corpus.cz
IČ: 25744616 DIČ: CZ25744616 Společnost Corpus Solutions a.s. je vedena u rejčířského soudu v Praze pod spisovou značkou B5936 Strana 100/190

Corpus Solutions a.s. Štikovská 1838/18 140 00 Praha 4
Tel: +420 241 020 333 E-mail: sales@corpus.cz Internet: www.corpus.cz
IČ: 25744616 DIČ: CZ25744616 Společnost Corpus Solutions a.s. je vedena u rejčířského soudu v Praze pod spisovou značkou B5936 Strana 100/190

IPv6 Multicast (MLDv1 & v2)		ANO
IPv6 Multicast (PIM SM)		ANO
IPv6 Multicast (PIM SSM)		ANO
IPv6 SLA nebo ekvivalentní technologie		ANO
uRPF pro IPv6		ANO
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels		ANO
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie		ANO
DHCPv6 Relay		ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking – DSCP, CoS		ANO
QoS Shaping and Policing		ANO
Class Based and Priority queuing		ANO
Rate Limiting		ANO
Hierarchical QoS	1 servisní	ANO
RSVP		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	50	ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)		ANO
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback)		ANO
IPSec AES 256		ANO
Hardwarová akcelerace šifrování pro IPSec AES 256		ANO
IKv2		ANO
SHA-2 (SHA-256, SHA-512)		ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT services)		ANO
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů		ANO
Pokročilá detekce a klasifikace jednotlivých přenesených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing		ANO
Měření statistik a výkonostních charakteristik přenesených multimediálních, reálnových a aplikačních toků - využíváme pásmo		ANO
Měření statistik a výkonostních charakteristik přenesených multimediálních, reálnových a aplikačních toků - odezvy aplikací		ANO

Měření statistik a výkonostních charakteristik přenesených multimediálních, reálnových a aplikačních toků - počty aplikačních spojení		ANO
Sběr a vyhodnocování statistik a výkonostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky		ANO
Monitorování aplikačních toků s využitím technologie NetFlow		ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvencí čísla, hodnota TTL, ICMP kód		ANO
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)		ANO
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX		ANO
Interní nástroje pro on-line měření kvality sítové infrastruktury, např. IP SLA nebo ekvivalentní		ANO
Interní nástroje pro debugging procházejícího provozu		ANO
Management		ANO
CLI rozhraní		ANO
SSHv2		ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL		ANO
SNMPv2		ANO
SNMPv3		ANO
Interpretace uživatelských CLI a Tel skriptů a jejich aktivace asynchronní události v systému zařízení		ANO
Čítače paketů pro jednotlivá pravidla v ACL		ANO
Sériová konzolová linka		ANO
DNS klient		ANO
NTP klient s MD5 autentizací		ANO
Administrátorem definovatelné monitory (sady statistik) sbírané o každém přeneseném paketu		ANO
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)		ANO
Statistiky exportovatelné pomocí NetFlow v9 (nebo IPFIX RFC 3957, RFC 3955)		ANO
Export detekované aplikace již daný "flow" náleží		ANO
Nástroje pro měření dynamických parametrů a odezvy v síti v libovolný okamžik, synteticky generovaným provozem (například IP SLA nebo ekvivalentní)		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO

Vzálehlý port mirroring napříč L3 doménou (např. ERSPAN nebo ekvivalentní)		ANO
Syslog		ANO
Služby		ANO
NTP server		ANO
DHCP server		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě záruky v průběhu celé pětileté záruky na dodaných zařízeních, kterou nemá Uchazeč schopen sám odstranit, bylo možné v režimě 8x24x7 tuto záruku eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému potřebných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu. V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochopitelné zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.19. Hraníční pobočkové směrovače

Pobočkový modulární směrovač s 5x 1Gb/s kombo RJ45/SFP porty. Směrovač slouží jako hraníční prvek pro redundantní WAN konektivitu. Směrovač řídí záložní datové toky a skrz WAN síť šifrované propojuje centrální kontrolér s distribučními prvky v jednotlivých řízených skupinách a virtualizovaných sítích.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 12	12ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní)	CI-CISCO4331/K9

produktové číslo nabízeného zařízení)		
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce		https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-43r/models.html
Požadovaná hodnota parametru	Minimální požadavky	Společně (ANO/NE)
Typ zařízení	Směrovač	ANO
Formát zařízení	Modulární	ANO
Požadovaný počet portů GigabitEthernet	5x10/100/1000 RJ45 a / a nebo SFP	ANO
Směrování IPv4		ANO
Směrování IPv6		ANO
OSPFv2		ANO
BGPv4		ANO
Podpora 4 byte AS numbers in BGP		ANO
Možnost směrování provozu dle dynamicky měřených metrik (zařízení linky, zpoždění, ztrátovost paketů, jitter)		ANO
First Hop Redundancy Protocol (např. VRRP, HSRP)		ANO
GRE (Generic Routing Encapsulation)		ANO
Policy-based routing podle ACL		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
IGMPv2, IGMPv3		ANO
uRPF		ANO
DHCP relay		ANO
First Hop Redundancy Protocol pro IPv6		ANO
OSPFv3		ANO
MP BGP		ANO
IPv6 Multicast (MLDv1 & v2)		ANO
IPv6 Multicast (PIM SM)		ANO
IPv6 Multicast (PIM SSM)		ANO
IPv6 SLA nebo ekvivalentní technologie		ANO
uRPF pro IPv6		ANO
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels		ANO
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie		ANO
DHCPv6 Relay		ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking – DSCP, CoS		ANO
QoS Shaping and Policing		ANO
Class Based and Priority queuing		ANO

Rate Limiting		ANO
Hierarchical QoS	1 úroveň	ANO
RSVP		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	100	ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING, VoIP gateway)		ANO
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback)		ANO
Stavový firewall		ANO
IPSec AES 256		ANO
Hardwarová akcelerace šifrování pro IPSec AES 256		ANO
Minimální propustnost směrovače při aktivovaných službách IPSec šifrování a QoS měřená pro IMIX provoz	700Mbps	ANO
IKEx2		ANO
SHA-2 (SHA-256, SHA-512)		ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)		ANO
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů		ANO
Pokročilá detekce a klasifikace jednotlivých přenesených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace shairing, policing		ANO
Měření statistik a výkonnostních charakteristik přenesených multimediálních, reálných a aplikačních toků - využívané pásmo		ANO
Měření statistik a výkonnostních charakteristik přenesených multimediálních, reálných a aplikačních toků - odezvy aplikací		ANO
Měření statistik a výkonnostních charakteristik přenesených multimediálních, reálných a aplikačních toků - počty aplikací spojení		ANO
Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky		ANO
Monitorování aplikačních toků s využitím technologie NetFlow		ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů zdrojová/cílová IP		ANO

adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód		
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)		ANO
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX		ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní		ANO
4G LTE záložní komunikační kanál		ANO
Interní nástroje pro debuging procházejícího provozu		ANO
SSHv2		ANO
CLI rozhraní		ANO
SNMPv2/v3		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
NTP server		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání softwaru, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění - tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě záduvy v průběhu celé pětileté záruky na dodávaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režimu RYSNBD tuto záduvu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze softwaru a operačního systému požadovaných zařízení přímo ze stránek výrobce na základě zaregistrovaní čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadávší pochýbnost zřejmá, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.20. Rozšiřující 10Gb karty

Originální rozšiřující karta s 16x 10Gb/s SFP+ porty pro Cisco Catalyst 6509E osazeným Supervisorem 2T. Karta umožňuje provoz minimálně 80Gb/s na sběrnici.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 3	3ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C6800-16P10G+
Odkaz na www stránku výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/je/ev/us/products/collateral/switches/catalyst-6800-series-switches/datasheet-c68-713666.html
Požadovaná hodnota parametru	Minimální Splněno požadavky (ANO/NE)
typ zařízení	vesilý vřid. modul switche ANO
Minimální počet 10Gb/s portů	16 ANO
Kompatibilní se šasi Cisco C6509E	ANO
Kompatibilní se supervisorem 2T a 2TXL	ANO
Rychlost komunikace se sběrnici	80 0Gb/s ANO

2.21. Rozšiřující servisní moduly

Originální supervizor kompatibilní do šasi Cisco Catalyst 6509E s minimální propustností 2Tb/s.

Základní údaje	Nabízená hodnota
Výrobce zařízení	CISCO
Počet kusů zařízení - 4	4ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	V5-52T-10G+
Odkaz na www stránku výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/je/ev/us/products/collateral/switches/modules/catalyst-6500-series-supervisor-cv3-line

Požadovaná hodnota parametru	Minimální požadavky	Splněno (ANO/NE)
Typ zařízení	řidic. modul switche	ANO
Celková minimální propustnost přepínacího subsystému	2 Tb/s	ANO
Přepínání IPv4 v Hardware	720 Mpps	ANO
Přepínání IPv6 v Hardware	390 Mpps	ANO
Minimální počet 128 000 záznamů v MAC adresní tabulce		ANO
Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	256000	ANO
Minimální počet záznamů ve směrovací tabulce - IPv6 unicast	128000	ANO
Minimální počet aktivních VLAN	4000	ANO
Řídicí modul s integrovanými rozhraními 10GE		ANO
Redundantní řídicí modul		ANO
Neměnná propustnost i při výpadku redundantního řídicího modulu		ANO
Funkční specifikace		ANO
Virtualizace - možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku - virtuálního šasi (jedná entita z hlediska L2 a L3 protokolů)		ANO
Ochranné mechanismy rozpadnutí virtuálního šasi bez nutnosti využití dodatečných zařízení		ANO
Podpora servisních modulů i v jednom virtuálním šasi sloučeném ze dvou fyzických		ANO
Stavové přepnutí mezi řídicími moduly v jednom fyzickém šasi (ekvivalent funkce Statefull Switchover/SSO)		ANO
Stavové přepnutí mezi řídicími moduly v logickém šasi (ekvivalent funkce Statefull Switchover/SSO mezi fyzickými šasi)		ANO
Směrování protokolů IPv4 a IPv6 v hardware (dualní podpora IPv4 a IPv6, tedy možnost současně konfigurovat IPv4 a IPv6 adres na totéž fyzické nebo logické rozhraní, dual-stack)		ANO
HW podpora MPLS a VPLS		ANO
Podpora tunelovacích protokolů (např. GRE) v hardware		ANO
Podpora překladu adres/NAT v hardware		ANO
Podpora standardu IEEE 802.3ad		ANO
Podpora IEEE 802.3ad přes více modulů		ANO
Podpora IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)		ANO
Minimální počet konfigurovatelných PortChannel trunků	100	ANO
Podpora IEEE 802.1Q		ANO
Podpora tunelování 802.1Q v 802.1Q		ANO

Podpora IEEE 802.1s - multiple spanning trees		ANO
Podpora IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Podpora IEEE 802.1p		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Hardwarová podpora dlouhých ethernetových rámců, tzv. "jumbo frames"		ANO
Detekce jednosměrnosti optické linky (např. UDLD)		ANO
Podpora QoS classification – dle ACL, IP Prec, DSCP, CoS		ANO
Podpora QoS marking – dle IP Prec, DSCP, CoS		ANO
Podpora QoS Policing		ANO
Podpora policingu na hodnotu agregovanou ze všech karet s lokálním přepínáním		ANO
Podpora policingu per-flow (např. microflow policing nebo funkčně ekvivalentní)		ANO
Podpora konfigurovatelných HW prostředků ochrany CPU před útoky typu DoS		ANO
Podpora hardwarové filtrace (access list) na fyzickém i logickém L2 i L3 rozhraní		ANO
Podpora hardwarové filtrace (access list) dle L2, L3 i L4 informací		ANO
Podpora hardwarové filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)		ANO
Podpora klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol dle RFC draft-smith-kandula-sxp-01 nebo funkčně ekvivalentní)		ANO
Podpora propagace bezpečnostní role uživatele nebo koncového zařízení pro laždy datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní)		ANO
HW podpora IEEE 802.1ae na 1 Gbit/s i 10 Gbit/s portech		ANO
Podpora zabezpečení a analýzy DHCP protokolu (např. DHCP snooping nebo funkčně ekvivalentní)		ANO
Podpora ochrany ARP protokolu (např. Dynamic ARP Inspection, DAI nebo funkčně ekvivalentní)		ANO
Podpora ochrany podvržené mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)		ANO
Podpora MPLS směrování		ANO
Podpora VPLS směrování		ANO
Podpora BGPv4, MP-BGP		ANO
Podpora OSPFv2, OSPFv3		ANO
Podpora OSPF s MD5 a NSSA		ANO

Podpora RIPv2, RIPv2		ANO
Podpora IS-IS podpora pro IPv4 a IPv6		ANO
Podpora Router Redundancy protokolu pro IPv4 (např. VRRP, HSRP)		ANO
Podpora Policy-based routing podle ACL		ANO
EIGRP (dle RFC draft-savage-eigrp-01)		ANO
Podpora PIM-SM (Protocol Independent Multicast, sparse mód)		ANO
Podpora PIM SSM (PIM Source Specific Multicast)		ANO
Podpora Bidirectional Protocol Independent Multicast (RFC 6015)		ANO
Podpora IGMPv2, IGMPv3		ANO
Podpora antispoofingové kontroly ekvivalentní funkci RPFC, reverse path forwarding check dle RFC3704 a RFC3178 pro IPv4 i IPv6		ANO
Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830)		ANO
Podpora IPv6 services (HTTP, DNS, SSH, ACL, ICMP, DHCP)		ANO
Podpora Router Redundancy protokolu pro IPv6 (např. VRRP, HSRP)		ANO
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard, Secure Neighbor Discovery)		ANO
Podpora IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)		ANO
Podpora IPv6 over GRE v hardware		ANO
Podpora ISATAP v hardware		ANO
Podpora IPv6 QoS		ANO
Možnost vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače/směrovače pro tvorbu VPN (podpora virtualizace směrovacích tabulek - např. funkčně ekvivalentní Virtual Routing and Forwarding / Multi-VRF)		ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)		ANO
NetFlow v9 (nebo IPIX RFC 3917, RFC 3955) a Flexible NetFlow (nebo funkčně ekvivalentní) pro IPv4 i IPv6		ANO
Podpora NetFlow (nebo funkčně ekvivalentní) na vstupu i vstupu		ANO
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů		ANO
Statistiky určované z každého paketu daného "flow"		ANO
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb		ANO
Návaznost skriptů interpretovaných přepínačem pro detekci daných parametrů "flow"		ANO
Zobrazení sbraných informací o "flow" přímo v přepínači. I včetně "TopN" pohledu.		ANO

Export statistik "flow" selektivně na více kolektorů		ANO
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní události v systému zařízení		ANO
Konfigurovatelná autodiagnostika při startu i za provozu zařízení		ANO
Podpora nástroje měření odezvy sítě (např. IP SLA) pro IPv4 i IPv6		ANO
Měření a ovládní spotřeby energie k LAN připojených koncových zařízení		ANO
Trasování media/aplikačních datových toků v celé síti a sběr statistik ze zařízení jimiž toky prochází		ANO
Textové řádkově orientované/CLI konfigurační rozhraní		ANO
Konfigurace zařízení v člověku čitelné textové formě		ANO
Možnost povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP		ANO
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP		ANO
Sériová konzolová linka		ANO
SSHv2		ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL		ANO
Podpora synchronizace času protokolem NTPv3 (klient i server)		ANO
SNMPv2		ANO
SNMPv3		ANO
L2 traceroute		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Podpora zrcadlení portů (funkční ekvivalent SPAN)		ANO
Podpora vzdáleného zrcadlení portů (funkční ekvivalent RSPAN)		ANO
Pokročilé interní nástroje pro ladění/debugging procházejícího provozu		ANO
Interní nástroje umožňující detailní analýzu a troubleshooting procházejících multimediálních datových toků, např. mediatrace nebo ekvivalentní		ANO
Podpora Syslog		ANO
DHCP server		ANO
NTP server		ANO

2.22. Propojovací moduly

25.

Základní údaje	Nabízená hodnota
----------------	------------------

QSFP 40-Gbps bidirectional short reach transceiver	
Výrobce zařízení	CISCO
Počet kusů - 60	60ks
Produktové číslo (typ) nabízeného zařízení	QSFP-40G-SR-BD
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-6608.html
10GBASE long reach SFP modul	
Výrobce zařízení	CISCO
Počet kusů - 240	240ks
Produktové číslo (typ) nabízeného zařízení	SFP-10G-LR-S
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-45289.html
10GBASE metalický SFP+ kabel 3 metry	
Výrobce zařízení	CISCO
Počet kusů - 8	8ks
Produktové číslo (typ) nabízeného zařízení	SFP-H10GB-CU3M
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-45289.html
10GBASE short reach SFP modul	
Výrobce zařízení	CISCO
Počet kusů - 8	8ks
Produktové číslo (typ) nabízeného zařízení	SFP-10G-SR-S
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-44764.html
QSFP 40-Gbps 4x 10G SFP+ Breakout cable 3m	
Výrobce zařízení	CISCO
Počet kusů - 4	4ks
Produktové číslo (typ) nabízeného zařízení	QSFP-40FP10G-CUSM
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-44764.html

/compatibility/matrix/4618_E_Dx_Matrix.html	
iGBASE-T RJ45 metalický SFP transceiver	
Výrobce zařízení	CISCO
Počet kusů - 13	13ks
Produktové číslo (typ) nabízeného zařízení	GLC-TS-
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/iGBASE-Tx_Matrix.html
10GBASE long reach SFP modul	
Výrobce zařízení	CISCO
Počet kusů - 10	10ks
Produktové číslo (typ) nabízeného zařízení	SFP-10G-ZR-S-
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GBase-Tx_Matrix.html
Třída zařízení optický transceiver	ANO
Formát zařízení-výměnný modul	ANO
Rychlost 10Gb	ANO
Dosah 80km	ANO
optický mód SFP	ANO
Vlnová délka světla 1550 nm	ANO
teplotní rozsah standard	ANO
konektor vlákna Dual LC/PC	ANO
konektor box GLC	ANO

3. Instalace a implementace Bepěného síťového prostředí

Dodavatel dále samostatně provede, dle závazného harmonogramu a schváleného postupu – analýzy Detailního návrhu řešení, tyto činnosti:

A.) Instalace zařízení v jednotlivých lokalitách

- o Bude postupováno dle Zadavatelem schváleného Detailního návrhu řešení
- o Bude postupováno dle Zadavatelem schváleného harmonogramu

B.) Implementaci řešení dle jednotlivých etap 3, až 8.

- o Bude postupováno dle Zadavatelem schváleného Detailního návrhu řešení
- o Bude postupováno dle Zadavatelem schváleného harmonogramu

A.) Instalace zařízení v jednotlivých lokalitách – seznam lokalit

Instalace do prostředí Zadavatele začne na základě akceptovaného a předaného Detailního návrhu řešení. Lokality, ve kterých bude probíhat implementace:

ID lokality	Název lokality	Adresa
BOH	DSA - STK Bohdalec	Nad Vřeskovou horou 88/4
BŘEV	DSA - STK Břevnov	Radimova 39, Praha 6
BUB	Archiv Bubny	Bubenská 8a
DC3	DC3 - VEGACOM	Lužná 4/591, Praha 6
DLM	Dům národních menšin	Vocelova 3, Praha 2
EMAU	OMI EMAUZY	Vyšehradská 55, Praha 2
CHP	MHMP - ZSP	Charvátova 9/145, Praha 1
JAR	DSA - STK Jarov / Osková	Ořkavá 2888/2, Praha 3
JUN	MHMP - Škodov palác	Jungmannova 25, Praha 1
GA	MHMP - Clam-Gallasov palác	Mariánské nám. 3
KCP	DSA - KCP (Kongresové Centrum Praha)	Na Pankráci 1685/17, Praha 4
MKP	Městská knihovna v Praze (MKP)	Mariánské nám. 1
NR	MHMP - Nová radnice	Mariánské náměstí 2, Praha 1
NUB	MHMP - Nová úřední budova	Nám. Frantze Kafky 1, Praha 1
OPLET	MHMP - Opletalova	Opletalova 22, Praha 1
RAE	MHMP Radniční blok (minuta)	U Radnice
REZ	MHMP - Primátorská rezidence	Mariánské nám. 1
RYT	MHMP Rytířská	Rytířská 10, Praha 1
STR	MHMP-Staroměstská radnice	Staroměstské náměstí 1/4
VAL	MHMP - Valentinská	Valentinská 4
VYS	DSA - STK Vysočany	Na výběžku 688/11, Praha 9

B.) Implementace dle jednotlivých etap

Etapa č. 3 – Migrace DC1

- v rámci této etapy dojde k vybudování nové infrastruktury paralelně vůči stávající DC infrastruktuře
- dojde k začlenění do stávající Cisco ACI infrastruktury v DC4
- bude nainstalován systém pro analýzu datových toků
- bude nainstalován systém pro ověřování uživatelů přistupujících do sítě MHMP
- bude nainstalován systém pro management aktivních prvků
- bude nainstalován systém SDN pro řízení přistupových přepínačů (DNA center)
- následně proběhnou testy funkčnosti
- poté budou migrovány servery a služby do nové infrastruktury
- dojde k začlenění bezpečného rozhraní pro analýzu síťového provozu do DC4 a DC5

Etapa č. 4 – Migrace lokality NUB

- v prvním kroku dojde k upgradu stávajících zařízení, které budou dále využívány v nové infrastruktuře
- následně dojde k přepojení přistupových přepínačů v lokalitě a zapojení do upgradovaných páteřních přepínačů

Etapa č. 5 – Migrace lokality JUN

- v prvním kroku bude zprovozněn pár páteřních přepínačů a ty budou propojeny do lokality NUB
- následně dojde k přepojení přistupových přepínačů v lokalitě a zapojení do nových páteřních přepínačů

Etapa č. 6 – Migrace lokalit WAN

- budou nainstalovány a zprovozněny centrální směrovače a agregátory šifrovaných spojení. Zařízení budou umístěna v DC1 a lokalitě NUB (nebo jiné momentálně vhodnější – např. DC4)
- v každé z migrovaných lokalit bude nejprve instalována bezpečnostní brána – směrovač a připojena k centrálním VPN agregátorům
- následně dojde k přepojení přistupových přepínačů v lokalitě a zapojení do nových směrovačů

Etapa č. 7 – Migrace lokalit FO

- v prvním kroku bude zprovozněn přepínač s přímým optickým propojením do lokality NUB
- bude nakonfigurováno zabezpečení optických linek protokolem 802.3ae
- následně dojde k přepojení přistupových přepínačů v lokalitě a zapojení do nových páteřních přepínačů

Etapa č. 8 – Migrace perimetru

- budou definovány vazby mezi připojením perimetr segmentů a novou částí infrastruktury
- proběhne rekonfigurace komunikačních tras
- proběhne přesun ISP konektivit do cílových umístění (DC3 a NUB – nebo dle aktuálních potřeb)
- bude nakonfigurována HA topologie mezi DC1 a mezi ISP
- bude provedena rekonfigurace stávajících bezpečnostních technologií

Testy

- budou provedeny akceptační testy
- budou provedeny záložové testy
- budou provedeny testy redundance

4. Úpravy konfigurací současných bezpečnostních technologií

V reakci na provedené úpravy v síti DC HMP bude nezbytné provést specifické úpravy ve stávajících součástech bezpečnostní infrastruktury HMP. Tyto změny budou znamenat zejména integraci již existujících bezpečnostních komponent s novými prvky sítě a napojení na nová poskytovaná rozhraní pro monitoring síťového provozu. Důležitou součástí je také zcela nová integrace nových síťových komponent do procesu šifru logů a bezpečnostního monitoringu.

- o Perimetrové firewally společnosti
- o Systémy řízení a sledování přístupů k síti, DDI a Network Visibility Module
- o Systémy aplikačního balancování a ochrany
- o Systém správy logů z provozní a bezpečnostní infrastruktury
- o Nástroje pro detekci a vyšetřování kybernetických incidentů
- o Nástroje pro správu bezpečnostních událostí SIEM

Tabulka detailních požadavků na dodávané řešení úpravy konfigurací současných bezpečnostních technologií:

Parametr	Požadovaná hodnota	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Perimetrové firewally společnosti Checkpoint	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: <ul style="list-style-type: none"> • Úpravě definic síťových segmentů • Změnách v bezpečnostní politice • Úpravách/změnách kabelového 	V rozsahu požadavků.	ANO

	zapojení zařízení		
Systémy řízení a sledování přístupů k síti, DDI a Network Visibility Module NOVICOM	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: <ul style="list-style-type: none"> Úpravě definic síťových segmentů Změnách v bezpečnostní politice Úpravách/změnách kabelového zapojení zařízení 	V rozsahu požadavků.	ANO
Systémy aplikačního balancování a ochrany F5	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: <ul style="list-style-type: none"> Úpravě definic síťových segmentů Změnách v balancovací a bezpečnostní politice Úpravách/změnách kabelového zapojení zařízení 	V rozsahu požadavků.	ANO
Systém správy logů z provozní a bezpečnostní infrastruktury LogManager	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: <ul style="list-style-type: none"> Úpravě definic síťových segmentů Změnách v konfiguraci logování Úpravách/změnách kabelového zapojení zařízení Zapojení dalších zdrojů logů 	V rozsahu požadavků.	ANO
Nástroje pro detekci a vyšetřování kybernetických incidentů FIDELIS	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: <ul style="list-style-type: none"> Úpravě definic síťových segmentů Úpravách/změnách kabelového zapojení zařízení Zapojení na nové rozhraní pro generování dat o síťovém provozu 	V rozsahu požadavků.	ANO
Nástroje pro správu bezpečnostních událostí SIEM IBM QRADAR	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: <ul style="list-style-type: none"> Úpravě definic síťových segmentů Úpravách/změnách kabelového zapojení zařízení Zapojení na nové rozhraní pro generování dat o síťovém provozu 	V rozsahu požadavků.	ANO

5. Poskytnutí služeb podpory výrobců technologie

zařízení v rámci dodávky jsou rozdělena do servisních kategorií, dle délky záruky a reakční doby na výpadek:

Kategorie	Počet měsíců záruky	SLA
Servisní skupina 1	6	8/5 NBD fix
Servisní skupina 2	8	8/5 NBD fix

Datum zahájení poskytování záruky je rovno datumu akceptace zařízení do provozu.

Podpora výrobce zahrnuje dostupnost:

- Upgrade, Update operačního systému a bezpečnostních aktualizací,
- Poskytování nových verzí a opravných balíčků SW, dle aktuální technologické úrovně,
- Výměna vadného dílu – odeslání NBD (následující pracovní den).

Druhy zařízení a servisní skupiny

Druh zařízení	Servisní skupina
Bezpečné rozhraní pro analýzu síťového provozu	Servisní skupina 1
Bezpečnostní hraniční brány firewall pro síť Mepnet	Servisní skupina 1
Centrální kontrolér LAN sítě	Servisní skupina 2
Monitorování datových toků	Servisní skupina 2
Řízení přístupu k síťovým prostředkům (802.1x)	Servisní skupina 2
Správa síťového prostředí	Servisní skupina 2
Datacentrové řešení Spine-Leaf	Servisní skupina 2
Spine vrstva	Servisní skupina 2
Leaf vrstva – 10GB SFP+	Servisní skupina 2
Leaf vrstva 10GB – RJ45	Servisní skupina 2
Leaf vrstva 1GB – RJ45	Servisní skupina 2
Next-Generation Firewall	Servisní skupina 2
Next-Generation Firewall	Servisní skupina 2
Virtuální privátní síť, vzdálené přístupy do sítě	Servisní skupina 2
Přístupové přepínače s 24 PoE porty	Servisní skupina 2
Distribuční přepínače	Servisní skupina 2
Přístupové přepínače s 48 PoE porty	Servisní skupina 2
Centrální přepínače	Servisní skupina 2
Agregační směrovač	Servisní skupina 2
Hraniční pobočkové směrovače	Servisní skupina 2
Rozšiřující 10GB karty	Servisní skupina 2
Rozšiřující servisní moduly	Servisní skupina 2
Propojovací moduly	Servisní skupina 2

6. Poskytnutí školení a servisní podpory spojené s provozem technologie

6.1. Školení pracovníků Zadavatele

- Předmětem veřejné zakázky je rovněž provedení školení pro administrátory Zadavatele k používání a správě technologií dodaných v rámci této veřejné zakázky.
- Školení 3 administrátorů v celkovém rozsahu 24 hodin/osoba. Školení musí proběhnout v sídle Zadavatele, certifikovaným pracovníkem.
- Za organizační zajištění školení zodpovídá dodavatel. Zadavatel zajistí pro školení bezplatné použití své počítačové učebny a zasedací místnosti.

6.2. Služby servisní podpory

- Podpora certifikovaného konzultanta a technika, pro řešenou oblast podpory
- Poskytování služeb HotLine/Helpdesk včetně servisní technické podpory dle parametrů SLA sjednaných touto Smlouvou. Příjem požadavků přes email, telefonní linku a webové rozhraní.
- Poskytování poradenských služeb prostřednictvím HotLine/Helpdesk při řešení běžných provozních problémů správců informačních systémů v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.

Řešení a kategorie vad:

- Vady kategorie A (kritická):**
Vady, které způsobují provozní problémy a neumožňují využívání systémů k účelu, jemuž jsou určeny.
- Vady kategorie B (vysoká):**
Méně závažné vady a nedostatky, které funkčně nebo kapacitně omezují využívání systémů k účelu, ke kterému jsou určeny.
- Vady kategorie C (střední a nízká):**
Vady a nedostatky, které neomezují využívání systémů k účelu, ke kterému jsou určeny, ale nejsou v souladu se správnou funkcí systému.

Garance	Vada kategorie A (režim 24x7)	Vada kategorie B (režim 8x5)	Vada kategorie C (režim 8x5)
Potvrzení příjmu požadavku a oznámení jména řešitele zákazníkovi	Do 30 minut od okamžiku nahlášení vady.	Do 30 minut od okamžiku nahlášení vady.	Do 1 hodiny od okamžiku nahlášení vady.

Vady mohou být nahlášené buď přes záznam v helpdesku poskytovatele, nebo hlášením z monitoringu proaktivně vedeného Poskytovatelem.

6.3. Zpracování dokumentace

- Součástí předání dokončeného díla bude elektronicky zpracovaná dokumentace a zakreslení skutečného provedení.

7. Poskytování dalších odborných služeb

Jedná se o další odborné služby nezahrnuté pod písm. a) či b) odst. 1.1 Smlouvy, které budou hrazeny na základě skutečně provedené práce vyjádřené v číselkovech.

- Školení dle požadavků Objednatele nad sjednaný rozsah.
- Konzultační podporu v rozsahu, ve kterém si Objednatel objedná.
- Součinnost při řešení systémových problémů systémů třetích stran.
- Součinnost při implementaci systémů třetích stran.
- Spolupráce při tvorbě koncepce dalšího rozvoje bezpečné sítě Objednatele.
- Spolupráce při koordinaci třetích stran.
- Jakékoliv úpravy a funkční doplnění projektu, nad rámec zadávací dokumentace, dle požadavků a pokynů Objednatele.

8. Harmonogram

Postup implementace

Zadavatel požaduje, aby dodavatel pracoval s projektovým řízením, dle jedné z obecně uznávaných metodik projektového řízení a pro celý průběh projektu bude stanoven řídicí výbor. Priority jednotlivých oblastí budou přezkoumány, dle aktuálních potřeb, neboť v některých lokalitách je situací zastaralých technologií nutné řešit přednostně. Etapy 6 až 8 lze realizovat v libovolném pořadí, v případě, že to zjiroje dovolí, lze také paralelně.

Návrh harmonogramu

Dokončení projektu bude provedeno do 12 měsíců od podpisu smlouvy s dodavatelem. Financování zakázky bude přizpůsobeno tomuto návrhu harmonogramu, tj. dílo bude financováno ve třech dílčích etapách. Jednotlivé etapy nemusí být realizovány v uvedeném pořadí, lze je přeuspořádat dle požadovaných priorit organizace.

Popis dílčího plnění	Termín zahájení	Termín ukončení
Zahájení a vypracování Detailního návrhu řešení (místní šetření a prováděcí projekt), dle etap 1 a 2.	T0	T0 + 1,5 měsíce = T1,5
Akceptace Detailního návrhu řešení zadavatelem	T1,5	T1,5 + 0,5 měsíc = T2
Dodávka softwarového a hardwarového vybavení počítačného k provozování všech požadovaných součástí dle etap 3, 4 a 5	T2	T2 + 1 měsíc = T3
Instalace a implementace technologií dle etap 3, 4 a 5	T3	T3 + 3 měsíce = T6
Upravy konfigurací současných bezpečnostní technologií dle potřeb nové síťové infrastruktury dle etap 3, 4 a 5	T2	T2 + 4 měsíce = T6
Dodávka softwarového a hardwarového vybavení počítačného k provozování všech požadovaných součástí, dle etap 6, 7 a 8	T6	T6 + 1 měsíc = T7
Instalace a implementace technologií dle etap 6, 7 a 8	T7	T7 + 3 měsíce = T10
Upravy konfigurací současných bezpečnostní technologií dle potřeb nové síťové infrastruktury dle etap 6, 7 a 8	T10	T10 + 1,5 měsíce = T11,5
Autorizované školení pracovníků zadavatele a zpracování dokumentace	T10	T10 + 2 měsíce = T12
Předání dokončeného díla a elektronicky zpracované dokumentace a zakreslení skutečného provedení	T11,5	T11,5 + 0,5 měsíce = T12
Služby podpory – záruky od výrobců technologie, skupina 1	T12	T12 + 36 měsíců = T48
Služby podpory – záruky od výrobců technologie, skupina 2	T12	T12 + 48 měsíců = T60
Poskytování technické podpory provozu dodavatelem. Podpora začíná běžet měsíc následující po předání díla – nejpozději T13.	T12	T12 + 36 měsíců = T48

Jednotlivé etapy jsou uvedeny v kalendářních měsících. To se rozumí den nabytí účinnosti Smlouvy.

9. Ostatní požadavky

Spotřební materiál a kabelážní systémy:

Součástí zakázky je také dodávka potřebného počtu všech propojovacích metalických i optických kabelů, vyřazovacích spojek a drobných úprav kabelážních systémů (např. posuny vyřazovacích panelů, pozic zařízení, atp. v rámci stávajícího datového rozvaděče, bez nutnosti porušení instalovaných optických a metalických van a patch panelů). Součástí dodávky není krimpování a vaření metalických či optických spojů do stávajících datových rozvaděčů.

V případě nabídky řešení SW formou tzv. virtual appliance (předkonfigurovaný virtuální image od výrobce daného řešení) je přípustný provoz na platformě VMware v existujícím prostředí Zadavatele, bez vicenákladů.

10. Součinnost zadavatele

- NON-IT zajištění prostor, do kterých bude nová technologie instalována
 - zálohované napájení/PDU
 - fyzický prostor v rariích
 - chlazení o dostatečném výkonu
- zajištění konektivity ve směru do WAN/LAN
 - kvalita linek odpovídající normám/smluvním ujednáním
 - patch kabely s příslušnými konektory odpovídající příslušným normám či standardům
 - ponechání stávajících optických/metalických modulů pro použití v cílovém stavu (mimo lokality DC)
- zajištění supportu pro stávající zařízení, které se zadavatel rozhodne ponechat
- zajištění soudčnosti externích dodavatelů MHMP

Příloha č. 2: Vzor Protokolu o předání a převzetí

IDENTIFIKACE

Zhotovitel	(Firma, IČO)
Objednatel	Hlavní město Praha, Mariánské náměstí 2/2, 110 01 Praha 1 IČO: 00064581
Zakázka (č. smlouvy Objednatele, název)	(č. smlouvy Objednatele) (Název)
Odpovědný pracovník Objednatele	(Jméno a příjmení)
Odpovědný pracovník Zhotovitele	(Jméno a příjmení)
Období	(měsíc/rok nebo od – do)

Předmět předání a převzetí

Datum	Specifikace (popis, kdo provedl)	Potvrzení garanta
[]		
(dd.mm.rrrr)		

Přehled předávané dokumentace

Č.	Název	Soubor

--	--	--

Dokumenty předány (komu, jak, kdy)

Schvalovací tabulka (v případě, že Objednatel nemá připomínky)

Subjekt	Pracovník role v zakázce/projektu	Datum	Podpis
Zhotovitel	Jméno a příjmení		
	Role		
Objednatel	Jméno a příjmení		
	Role		

Oprávněné osoby dle smlouvy

Příloha č. 3: Vzor Akceptačního protokolu

AKCEPTAČNÍ PROTOKOL

PROJEKT

Identifikace projektu	
Název projektu	
Zkratka	
Vedoucí projektu za Objednatele	
Zpracovatel protokolu	
Číslo protokolu	

PŘEDMĚT AKCEPTACE

Smlouva / číslo	<i>přípř. jiný dokument, na základě jehož k akceptaci dochází</i>
Předmět dodávky, plnění (podle smlouvy)	<i>např. služba, aplikace, dokumenty (např. konkrétní)</i>
Důvod akceptace	<i>např. ukončení etapy, dokončení milníku</i>
Forma akceptace	<i>např. předání dokumentace, CD s aplikací, spuštění aplikace,...</i>

SMLUVNÍ STRANY

OBJEDNATEL	
Název	Hlavní město Praha

Adresa	Mariánské náměstí 2/2, 110 01 Praha 1
IČO	000 64 581
Odpovědná osoba	<i>osoba uvedená ve smlouvě</i>
Funkce	
ZHOTOVITEL	
Název	<i>Dle smlouvy</i>
Adresa	
IČO	
Odpovědná osoba	<i>osoba uvedená ve smlouvě</i>
Funkce	

SEZNAM PŘÍLOH

Typ přílohy (manuál, CD, ...)	Název	Označení přílohy (číslo, název souboru)	Zodpovědná osoba (kdo je zodpovědný za přílohu)	Doplňující informace
1.				
2.				
3.				

SEZNAM ZÁVAD

Č.	ZÁVADA	Popis závady	Termín odstranění	Osoba, zodpovědná za odstranění závady
1.				
2.				

Fo odstranění závady proběhne nová akceptační procedura.

ZÁVĚR AKCEPTACE (hodící se zkratkou)

<input type="checkbox"/>	Při akceptaci nebyly zjištěny závady.
<input type="checkbox"/>	Při akceptaci byly zjištěny závady, jejichž seznam a popis je uveden v příloze. Tyto závady NEBRÁNÍ akceptaci.
<input type="checkbox"/>	Při akceptaci byly zjištěny závady, jejichž seznam a popis je uveden v příloze. Tyto závady BRÁNÍ akceptaci.

SCHVALOVACÍ TABULKA

OBJEDNATEL	Jméno a příjmení	Datum	Podpis
Vedoucí projektu			
Projektový konzultant	<i>pokud je určen</i>		
Teamový koordinátor PK	<i>pokud je určen</i>		
Oprávněná osoba uvedená ve smlouvě	<i>např. Člen vedení</i>		

ZHOTOVITEL	Jméno a příjmení	Datum	Podpis
Vedoucí projektového týmu zhotovitele			
Oprávněná osoba uvedená ve smlouvě			

Příloha č. 4: Harmonogram plnění

Popis dílčího plnění	Termín zahájení	Termín ukončení
Zahájení a vypracování Detailního návrhu řešení (místní šetření a prováděcí projekt), dle etapy 1 a 2.	T0	T0 + 1,5 měsíce = T1,5
Akceptace Detailního návrhu řešení zadavatelem	T1,5	T1,5 + 0,5 měsíce = T2
Dodávka softwarového a hardwarového vybavení potřebného k provozování všech požadovaných součástí, dle etap 3, 4 a 5	T2	T2 + 1 měsíc = T3
Instalace a implementace technologií dle etapy 3, 4 a 5	T3	T3 + 3 měsíce = T6
Úpravy konfigurací současných bezpečnostních technologií dle potřeb nové síťové infrastruktury dle etapy 3, 4 a 5	T2	T2 + 4 měsíce = T6
Dodávka softwarového a hardwarového vybavení potřebného k provozování všech požadovaných součástí, dle etap 6, 7 a 8	T6	T6 + 1 měsíc = T7
Instalace a implementace technologií dle etapy 6, 7 a 8	T7	T7 + 3 měsíce = T10
Úpravy konfigurací současných bezpečnostních technologií dle potřeb nové síťové infrastruktury dle etapy 6, 7 a 8	T10	T10 + 1,5 měsíce = T11,5
Autorizované školení pracovníků zadavatele a zpracování dokumentace	T10	T10 + 2 měsíce = T12
Předání dokončeného díla a elektronicky zpracované dokumentace a zakreslení skutečného provedení	T11,5	T11,5 + 0,5 měsíce = T12
Služby podpory – záruky od výrobců technologie, skupina 1	T12	T12 + 36 měsíců = T48
Služby podpory – záruky od výrobců technologie, skupina 2	T12	T12 + 48 měsíců = T60

Poskytování technické podpory provozu dodavatelem. Podpora začíná běžet měsíc následující po předání díla – nejpozději T13.	T12	T12 + 36 měsíců = T48
---	-----	-----------------------

Jednotlivé etapy jsou uvedeny v kalendářních měsících. To se rozumí den nabytí účinnosti Smlouvy.

Příloha č. 5: Podrobná specifikace ceny

Ceny doplní dodavatel dle přílohy č. 5 zadávací dokumentace

A. Dodávka detailního návrhu řešení a technologií, včetně instalace a implementace

a. FÁZE 1

Položka č.	Dílčí plnění	Množství (ks)	Cena za ks v Kč bez DPH	Cena v Kč bez DPH
1	Vypracování Detailního návrhu řešení, dle etapy 1 a 2.	1	500 000,-	500 000,00 Kč
2	Dodávka technologií pro Bezpečné síťové prostředí, dle etapy 3 a 4.	1	35 920 750,-	35 920 750,00 Kč
3	Instalace a implementace zařízení v jednotlivých lokalitách, dle etapy 5 a 6.	1	5 800 000,-	5 800 000,00 Kč
4	Služby úpravy konfigurační současných bezpečnostní technologií, dle etapy 7 a 8.	1	2 500 000,-	2 500 000,00 Kč
Cena celkem v Kč bez DPH				44 720 750,- Kč

a. FÁZE 2

Položka č.	Dílčí plnění	Množství (ks)	Cena za ks v Kč bez DPH	Cena v Kč bez DPH
5	Dodávka technologií pro Bezpečné síťové prostředí, dle etapy 6 a 8.	1	51 199 448,-	51 199 448,00 Kč
6	Instalace a implementace zařízení v jednotlivých lokalitách, dle etapy 6 a 8.	1	4 200 000,-	4 200 000,00 Kč
7	Služby úpravy konfigurační současných bezpečnostní technologií, dle etapy 6 a 8.	1	2 600 000,-	2 600 000,00 Kč
Cena celkem v Kč bez DPH				57 999 448,- Kč

B. Dodávka služeb podpory výroby, školení a služeb podpory provozu

Položka č.	Dílčí plnění	Množství (ks)	Cena za ks v Kč bez DPH	Cena v Kč bez DPH
8	Služby záruky a podpory výrobce technologie	1	26 029 802,-	26 029 802,00 Kč
9	Služby servisní podpory spojené s provozem technologie	1	1 000 000,-	1 000 000,00 Kč
10	Školení pracovníků zadavatele pro administrátorův a zpracování dokumentace*	1	100 000,-	100 000,00 Kč
Cena celkem v Kč bez DPH				27 129 802,- Kč

Cena celkem (A+B) v Kč bez DPH 129 830 000,00 Kč

*Předání elektronicky zpracované dokumentace a zakrštění skutečného provedení.

C. Poskytování dalších odborných služeb

Dílčí plnění	Cena za 1 člověka-rok v Kč bez DPH	Cena 1 člověka-rok v Kč bez DPH
Cena za 1 člověka-rok poskytování dalších odborných služeb	12 500,- Kč	12 500,00 Kč

Příloha č. 6: Nabídka Zhotovitele

(zde bude Objednatelům vložena nabídka Zhotovitele)

Příloha č. 7:
Seznam členů realizačního týmu

Pozice člena týmu	Kontaktní údaje	Certifikace
Hlavní projektový manažer		PRINCE 2
Specialista architekt řešení		TOGAF 9
Specialista řízení IT služeb		ITIL
IT specialista bezpečnosti		CISSP
IT specialista na bezpečnostní technologii – LAN		CCIE Routing&Switching
IT specialista na bezpečnostní technologii – LAN		CCIE Routing&Switching

IT specialista na bezpečnostní technologii – FIREWALL FS		FS Professional
IT specialista na bezpečnostní technologii – FIREWALL FS		FS Professional
IT specialista na bezpečnostní technologii – FIREWALL CHECKPOINT		Check Point Certified Security Master
IT specialista na bezpečnostní technologii – FIREWALL CHECKPOINT		Check Point Certified Security Expert
IT specialista na bezpečnostní technologii – SIEM QRADAR		IBM Certified Associate Administrator/ Security Qradar SIEM V7.2.8
IT specialista na bezpečnostní technologii – SIEM QRADAR		Osvědčení o způsobilosti dle vyhlášky č.50/1978 Sb.
IT specialista na bezpečnostní technologii – SIEM QRADAR		IBM Certified Associate Administrator/ Security Qradar SIEM V7.2.8
IT specialista na bezpečnostní technologii – SIEM QRADAR	Jméno a příjmení: [redacted]	NOVICOM

technologie – NOVICOM		
IT specialista na bezpečnostní technologii – NOVICOM		NOVICOM
IT specialista na bezpečnostní technologii – FIDELIS		FIDELIS
IT specialista na bezpečnostní technologii – FIDELIS		FIDELIS
IT specialista pro serverovou infrastrukturu - VMware		VMware Certified Professional 6 Data Center Virtualization
IT specialista pro serverovou infrastrukturu - VMware		VMware Certified Professional 6 Data Center Virtualization
IT specialista na síťovou virtualizaci – SDN		CCIE Routing&Switching
IT specialista na síťovou virtualizaci – SDN		CCIE Routing&Switching

Požadavky na členy realizačního týmu

Zhotovitel v seznamu členů realizačního týmu zakázky uvede tyto pozice:

- A) hlavní projektový manažer (1 osoba),
- B) specialista architekt řešení (1 osoba),
- C) specialista řízení IT služeb (1 osoba),
- D) specialista bezpečnosti (1 osoba),
- E) IT specialista na bezpečnostní technologii – LAN (2 osoby),
- F) IT specialista na bezpečnostní technologii – Firewall FS (2 osoby),
- G) IT specialista na bezpečnostní technologii – Firewall Checkpoint (2 osoby),
- H) IT specialista na bezpečnostní technologii – SIEM QRADAR (2 osoby),
- I) IT specialista na bezpečnostní technologii – NOVICOM (2 osoby)
- J) IT specialista na bezpečnostní technologii – FIDELIS (2 osoby)
- K) IT specialista – Virtualizace serverů – VMware (2 osoby),
- L) IT specialista na virtualizaci sítí – SDN (2 osoby),

Objednatel požaduje, aby jakýkoli (alespoň jeden) člen týmu byl držitelem platné osvědčení o způsobilosti dle vyhlášky č. 50/1978 Sb. – doložením kopie dokladu osvědčující tuto způsobilost.

Odborné technické certifikáty a doklady prokazující vzdělání budou akceptovány v českém, slovenském nebo anglickém jazyce.

Jedna fyzická osoba může zastávat více pozic v týmu, s výjimkou osob splňujících požadavky dle A až J (u kterých je požadavek, aby tyto osoby nezastávaly jinou pozici v týmu).

Doklad prokazující vzdělání a certifikace k pozici Projektový manažer



OZNACENÍ ROLE	Hlavní projektový manažer
Požadované minimální vzdělání	Ukončené vysokoškolské vzdělání v magisterském studijním programu
Požadované certifikace	Platná certifikace v oblasti projektového řízení nebo technickou certifikaci v oblasti informačních technologií, např. Certifikaci PMI, IPMA, Prince 2, CompTIA Project+ nebo jiné ekvivalentní
Požadované znalosti a praxe	Profesní zkušenost z vedením alespoň 2 projektů spočívajících v instalaci, zprovoznění a konfiguraci SIEM systémů a aplikací stejného nebo obdobného rozsahu jako je předmět plnění této veřejné zakázky, a to na pozici hlavního projektového manažera nebo obdobné pozici, která měla odpovědnost po stránce realizace projekt řídit a vést
Další podmínky	Kopie platného certifikátu prokazující požadované minimální vzdělání a držení požadované certifikace musí být připojena na následující stranách

Osoba nominovaná na tuto roli uvedené požadavky splňuje.



ČESKÁ REPUBLIKA
Význam
DIPLOM
Vydáno AA 078426 C. 1687



OZNACENÍ ROLE	Specialista architekt řešení
Požadované minimální vzdělání	Ukončené vysokoškolské vzdělání v magisterském studijním programu
Požadované certifikace	Platná certifikace v oblasti návrhu a architektury informačních technologií, např. TOGAF, IASA Associate, CITA-P (Certified Information Technology Architect Professional Certification) nebo jiné ekvivalentní
Požadované znalosti a praxe	Profesní zkušenost s minimálně 2 projekty s obdobným předmětem plnění, tj. návrh a implementace řešení SIEM, tj. stejným nebo obdobným jako je předmět této veřejné zakázky
Další podmínky	Kopie platného certifikátu prokazující požadované minimální vzdělání a držení požadované certifikace musí být připojena na následujících stranách

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující vzdělání a certifikace k pozici Specialista architekt řešení



This is to certify that

has successfully met the requirements of the TOGAF 9 Certification for People program at the TOGAF 9 Certified level.

Date registered: 4 March 2014
Registration Number

The Open Group

TOGAF and The Open Group certification logo are trademarks of The Open Group. The certification logo may only be used on or in connection with those products, persons, or organizations that have been certified under this program. The certification register may be viewed at <http://www.opengroup.org/logo/certregister.html>

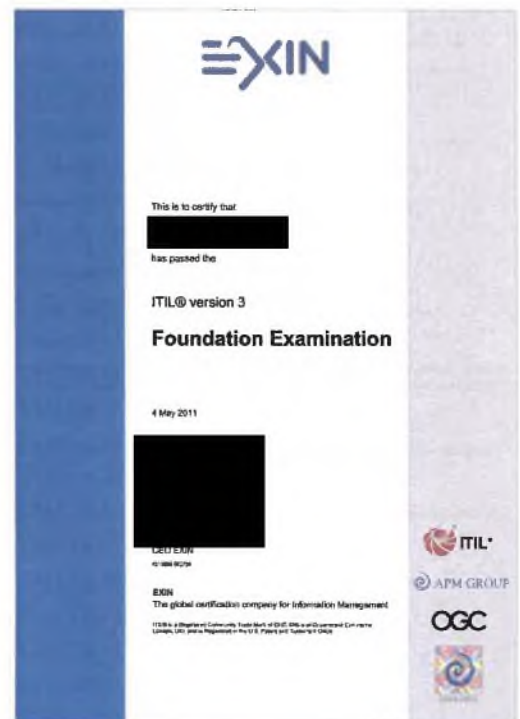
© Copyright 2014 The Open Group. All rights reserved.



OZNAČENÍ ROLE	Specialista řízení IT služeb
Požadované minimální vzdělání	Ukončené vysokoškolské vzdělání v magisterském studijním programu
Požadované certifikace	Platná certifikace v oblasti řízení a správu IT služeb, např. ITIL, COBIT, ISO 20000 auditor
Požadované znalosti a praxe	Profesní zkušenost s minimálně 2 projekty s obdobným předmětem plnění jako je předmět této Smlouvy, a to na pozici specialista řízení IT služeb nebo jiné ekvivalentní systémy pro mezinárodně uznávaný a rozšířený standard pro řízení a správu IT služeb
Další podmínky	Kopie platného certifikátu prokazující požadované minimální vzdělání a držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující vzdělání a certifikace k pozici Specialista řízení IT služeb



Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie LAN



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologie – LAN- 2
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na produkty LAN
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci LAN sítě po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Corpus Solutions a.s.
Štěrbaňská 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiškového soudu
v Praze pod spisovou značkou B5936

Strana 149/190

Corpus Solutions a.s.
Štěrbaňská 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiškového soudu
v Praze pod spisovou značkou B5936

Strana 150/190

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie LAN



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologie – F5 - 1
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na bezpečnostní produkty F5
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci zabezpečení sítě po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Corpus Solutions a.s.
Štěrbaňská 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiškového soudu
v Praze pod spisovou značkou B5936

Strana 151/190

Corpus Solutions a.s.
Štěrbaňská 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiškového soudu
v Praze pod spisovou značkou B5936

Strana 152/190

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie F5



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologie – F5 - 2
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na bezpečnostní produkty F5
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci zabezpečení sítě po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Corpus Solutions a.s.
Sokolova 1538/18
140 00 Praha 4

Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25744616
DIČ: CZ25744616
Společnost Corpus Solutions a.s. je veškerá o registrace součástí
v Praze pod spornou značkou B373a

Strana 153/190

Corpus Solutions a.s.
Sokolova 1538/18
140 00 Praha 4

Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25744616
DIČ: CZ25744616
Společnost Corpus Solutions a.s. je veškerá o registrace součástí
v Praze pod spornou značkou B373a

Strana 154/190

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie F5



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologie – Checkpoint - 3
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na bezpečnostní produkty Checkpoint
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci zabezpečení sítě po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Corpus Solutions a.s.
Sokolova 1538/18
140 00 Praha 4

Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25744616
DIČ: CZ25744616
Společnost Corpus Solutions a.s. je veškerá o registrace součástí
v Praze pod spornou značkou B373a

Strana 153/190

Corpus Solutions a.s.
Sokolova 1538/18
140 00 Praha 4

Tel: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25744616
DIČ: CZ25744616
Společnost Corpus Solutions a.s. je veškerá o registrace součástí
v Praze pod spornou značkou B373a

Strana 154/190

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologii Checkpoint



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologii – Checkpoint - 2
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na bezpečnostní produkty Checkpoint
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci zabezpečení sítě po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologii Checkpoint



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologii – QRADAR SIEM - 1
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na bezpečnostní produkty QRADAR
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci zabezpečení SIEM systémů QRADAR po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologii IBM QRADAR SIEM



OZNAČENÍ ROLE:	IT specialista na bezpečnostní technologii – QRADAR SIEM - a
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace na bezpečnostní produkty QRADAR
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci zabezpečení SIEM systémů QRADAR po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologii IBM QRADAR SIEM



OZNACENÍ ROLE	IT specialista na bezpečnostní technologie – NOVICOM - 1
Požadované minimální vzdělání	-
Požadované certifikace	Platnou certifikaci na produkt Detekce a správy zranitelnosti v oblasti bezpečnostních informačních technologií - NOVICOM
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci systémů pro zabezpečení systémů po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie – NOVICOM



OZNACENÍ ROLE	IT specialista na bezpečnostní technologie – NOVICOM - 2
Požadované minimální vzdělání	-
Požadované certifikace	Platnou certifikaci na produkt Detekce a správy zranitelnosti v oblasti bezpečnostních informačních technologií - NOVICOM
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci systémů pro zabezpečení systémů po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie – NOVICOM



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologie – FIDELIS - 1
Požadované minimální vzdělání	-
Požadované certifikace	Platnou certifikaci na produkt Detekce a správy zranitelnosti v oblasti bezpečnostních informačních technologií - FIDELIS
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci systémů pro zabezpečení systémů po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie – FIDELIS



OZNAČENÍ ROLE	IT specialista na bezpečnostní technologie – FIDELIS - 2
Požadované minimální vzdělání	-
Požadované certifikace	Platnou certifikaci na produkt Detekce a správy zranitelnosti v oblasti bezpečnostních informačních technologií - FIDELIS
Požadované znalosti a praxe	Profesní zkušenost v oblasti spočívajících v instalaci, zprovoznění a konfiguraci systémů pro zabezpečení systémů po dobu nejméně 2 let v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultacích
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na bezpečnostní technologie – FIDELIS



OZNAČENÍ ROLE	IT specialista na serverové virtualizace
Požadované minimální vzdělání	-
Požadované certifikace	Platné certifikaci v oblasti informačních technologií se zaměřením na produkty VMware verze 6 a vyšší
Požadované znalosti a praxe	Profesní zkušenost v oblasti serverových operačních systémů a virtualizací po dobu nejméně 1 roku v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultaci v oblasti serverových virtualizace OS na platformě Windows
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista na serverové virtualizace

vmware

VMware is proud to award the title of
VMware Certified Professional 6
Data Center Virtualization

to

in recognition of successful completion
of all certification requirements

VMware Certified Professional 6
Data Center Virtualization

VMware Certified Professional 6

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiřského soudu
v Praze pod spisovou značkou B5936

Strana 173/190

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiřského soudu
v Praze pod spisovou značkou B5936

Strana 174/190

OZNAČENÍ ROLE	IT specialista na serverové virtualizace
Požadované minimální vzdělání	-
Požadované certifikace	Platné certifikaci v oblasti informačních technologií se zaměřením na produkty VMware verze 6 a vyšší
Požadované znalosti a praxe	Profesní zkušenost v oblasti serverových operačních systémů a virtualizací po dobu nejméně 1 roku v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci anebo technických konzultaci v oblasti serverových virtualizace OS na platformě Windows
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

vmware

VMware is proud to award the title of
VMware Certified Professional 6
Data Center Virtualization

to

in recognition of successful completion
of all certification requirements

VMware Certified Professional 6
Data Center Virtualization

VMware Certified Professional 6

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiřského soudu
v Praze pod spisovou značkou B5936

Strana 175/190

Corpus Solutions a.s.
Sokolova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s. je vedena u rejdiřského soudu
v Praze pod spisovou značkou B5936

Strana 176/190

OZNAČENÍ ROLE	IT specialista pro systémy LAN SDN
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace v oblasti informačních technologií se zaměřením na síťové prvky LAN a tzv. Software Defined Networking
Požadované znalosti a praxe	Profesní zkušenost na pozici systémového inženýra pro oblast LAN infrastruktury po dobu nejméně 1 roku v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci, technických konzultacích síťových prvků LAN - SDN
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista pro systémy LAN SDN



OZNAČENÍ ROLE	IT specialista pro systémy LAN SDN
Požadované minimální vzdělání	-
Požadované certifikace	Platná certifikace v oblasti informačních technologií se zaměřením na síťové prvky LAN a tzv. Software Defined Networking
Požadované znalosti a praxe	Profesní zkušenost na pozici systémového inženýra pro oblast LAN infrastruktury po dobu nejméně 1 roku v rámci projektů spočívajících v dodávce, instalaci, zprovoznění, základní a pokročilejší konfiguraci, technických konzultacích síťových prvků LAN - SDN
Další podmínky	Kopie platného certifikátu prokazující držení požadované certifikace musí být připojena na následující straně

Osoba nominovaná na tuto roli uvedené požadavky splňuje.

Doklad prokazující certifikace k pozici IT specialista pro systémy LAN SDN



Příloha č. 8: Vzor Výkazu plnění a protokol o převzetí plnění

	HLAVNÍ MĚSTO PRAHA MAGISTRÁT HLAVNÍHO MĚSTA PRAHY ODBOR INFORMATIKY
	Výkaz plnění a protokol o převzetí plnění

PROJEKT

Identifikace projektu	
Název projektu	Bezpečné síťové prostředí
Zkratka	
Vedoucí projektu za HMP	
Zpracovatel protokolu	
Číslo protokolu	

PŘEDMĚT PŘEDÁNÍ PŘEVZETÍ

Smlouva / číslo	popř. jiný dokument, na základě jehož k akceptaci došlo
Předmět, plnění	popř. služba, aplikace, dokumenty (popř. konkrétní)
Důvod akceptace	popř. ukončení etapy, dokončení projektu
Forma akceptace	popř. předání dokumentace, CD s aplikací, spuštění aplikace...

SMLUVNÍ STRANY

OBJEDNATEL	
Název	Hlavní město Praha
Sídlo	Mariánské nám. 2, Praha 1, PSČ: 110 01
IČO	00064581
Odpovědná osoba	osoba uvedená ve smlouvě

Funkce	
ZHOTOVITEL	
Název	Dle smlouvy
Adresa	
IČO	
Odpovědná osoba	osoba uvedená ve smlouvě
Funkce	

SEZNAM POSKYTNUTÝCH SLUŽEB

	Popis poskytnutých služeb	Doplňující informace
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

SCHVALOVACÍ TABULKA

OBJEDNATEL	Jméno a příjmení	Datum	Podpis
Vedoucí projektu			
Projektový konzultant	popř. je určen		
Teamový koordinátor PK			
Oprávněná osoba uvedená ve smlouvě	popř. člen vedení odboru MHP-INF		

ZHOTOVITEL	Jméno a příjmení	Datum	Podpis
Oprávněná osoba uvedená ve smlouvě			

Identifikační údaje poddávatele

Obchodní jméno	ALEF NULA s.s.
Sídlo společnosti	Pernéřova 691/42, Karlín, 186 00 Praha
Právní forma společnosti	Akčiová společnost zapsaná v obchodním rejčířku vedeném u Městského soudu v Praze, sp. zn. B 2727
IČ	61858579

PÍSEMNÝ ZÁVAZEK JINÉ OSOBY

Věřejná zakázka: „Bezpečné síťové prostředí“ v rámci ČÁSTI I Dodávky HW zařízení a standardního SW dynamického sdíleního systému a návrh „Dodávky HW zařízení, standardního SW a odborných služeb technického poskytovatel“ („Věřejný zážitek“)

Zadavatel: Hlavní město Praha, se sídlem Mariánské náměstí 22, 110 01 Praha 1, IČO: 00064581 („Zadavatel“)

Společnost ALEF NULA, s.s. se sídlem Pernéřova 691/42, Karlín, 186 00 Praha 8, IČO: 61858579, zapsaná v obchodním rejčířku vedeném u Městského soudu v Praze, sp. zn. B 2727, specializuje se na bezpečné síťové prostředí („Prostředí bezpečí“), jakžto jiná osoba, poskytovatel, který dodává v rámci této zakázky „Věřejný zážitek“ („Zadavatel“), poskytuje technickou kvalifikaci (dle čl. 7.3 smlouvy) dokumentovanou Věřejným zážitkem, se kterým je srovnáno § 83 odst. 1 písm. d) zákona č. 134/2016 Sb., o podmínkách veřejných zakázek, zveřejněno 16. srpna, že v případě uzavření smlouvy na plnění Věřejného zážitku mezi Zadavatelem a Dodavatelem, se bude na plnění předmětu Věřejného zážitku podílet minimálně v rozsahu, který odpovídá ze Dodavatele poskytnuté kvalifikaci. Jedná se o tyto činy realizované tj.:

- Specialista architektury řešení
- IT specialista na bezpečnostní technologie – LAN - 1
- IT specialista na bezpečnostní technologie – LAN - 2
- IT specialista pro systémy LAN SDN - 1
- IT specialista pro systémy LAN SDN - 2
- IT specialista na serverové virtuálizace - 2

Poddávatel se tímto neodvolatelně a neprovdělně zavazuje § 83 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zavazuje se své společnosti a nerozšířit odpovědnost za plnění Věřejného zážitku společně s Dodavatelem a dále odlišně a odděleně Dodavatel ze vkladový úrok, úroky, náklady, škody, nemajetkovou újmu nebo výdaje (včetně, nikoliv však výše uvedených, částky uzavřené na základě soudních rozhodnutí, soudě a rozhodnutí, jakžto vzhledem ke právní zárukou nebo jiných nákladů a výdajů vyžadovaných nebo obdržely vzhledem k úhradě nebo uzavření smlouvy) poskytnout, které Dávatelovi vzniknou, přijdou-li a, nebo vzniklé v souvislosti s, poskytnutím činnosti Poddávatele nebo v souvislosti s ním.

V Praze, dne 29. 6. 2018

ALEF NULA
ALEF NULA, s.s.
Pernéřova 691/42, Karlín, 186 00 Praha 8
IČ: 61858579 DIČ: CZ61858579

Písemný závazek Poddávatele v rozsahu popsaném výše akceptuji.

V Praze, dne: 27. 6. 2018

CORPUS SOLUTIONS
Corpus Solutions s.s.
Štáblova 1638/18
140 00 Praha 4
IČ: 25764616 DIČ: CZ25764616 Společnost Corpus Solutions s.s. je vedena u rejčířského soudu v Praze pod spisovou značkou 65936

za Uplatnění

Plná moc

Název: ALEF NULA, a.s.
Adresa: Pernerova 69/42, 186 00 Praha 8
Zastupující / jednající: [redacted] předseda představenstva a
IČ: 61858579

limto zmocňuje

Jméno: [redacted]
Bytem: [redacted]
Datum naryzení: [redacted]
Funkce v organizaci / značení: [redacted]
Umožnění:

Číslo a obsah: [redacted]

Handwritten note: "Všechny souhlasím, neproblemy poskytnout sítě"
"provozovat" "zadání, které Hlavou máte před."

V Praze dne 29. 6. 2018

V Praze dne 29. 6. 2018

Tato plná moc platí do: 30. 6. 2018

ALEFNULA, a.s.
Pernerova 69/42, 186 00 Praha 8
IČ: 61858579

ALEF NULA, a.s.
Pernerova 69/42, 186 00 Praha 8
IČ: 61858579

5 Další doklady a dokumenty

5.1 Doklady o poddávatele

5.1.1 Identifikační údaje poddávatele

Table with 2 columns: Obchodní jméno, Sídlo společnosti, Právní forma společnosti, IČ. Values include ALEF NULA, a.s., Pernerova 69/42, Karlín, 186 00 Praha, Akciová společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. B 2727, 61858579.

5.1.2 Činnosti realizované poddávatelem

Dodavatel bude realizovat část zakázky pomocí subdávatele a to v rozsahu níže uvedených rolí:

- Specialista architekt řešení
IT specialista na bezpečnostní technologie – LAN- 1
IT specialista na bezpečnostní technologie – LAN- 2
IT specialista pro systémy LAN SDN - 1
IT specialista pro systémy LAN SDN - 2
IT specialista na serverové virtualizace - 2

5.1.3 Písemný závazek poddávatele

PÍSEMNÝ ZÁVAZEK JINÉ OSOBY

Vytvářející zakázka: „Bezpečnostní úložiště“ v rámci „ČÁSTI I Dodávky HW zařízení a instalace SW dynamického síťového systému a úložiště „Diskový I/O zařízení, standardizováno SW a ucelených služeb technického podpora“ („Všechny zakázky“)

Zadavatel: Hlavní město Praha, se sídlem Mělnická náměstí 27, 118 01 Praha 1, IČ: 00064581 („Zadavatel“)

Společnost ALEF NULA, a.s. se sídlem Pernerova 69/42, Karlín, 186 00 Praha 8, IČ: 61858579, zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. B 2727, specializuje se na bezpodmínečné provádění („Poddávatele“), jmenovitě jako specialista, poskytovatel služeb dodavatel Corpus Solutions a.s., se sídlem Sokolova 1636/18, 140 00 Praha 4, IČ: 25764616 („Dodavatel“), prožádá technickou kvalifikaci dle čl. 7.5 zadávací dokumentace Všechny zakázky, se kterou ve vztahu k čl. 81 odst. 1 písm. d) zákona č. 134/2016 Sb., o způsobech výběru veřejných zakázek, závazuje se tím, že v případě uzavření smlouvy na plnění veřejné zakázky mezi Zadavatelem a Dodavatelem, se bude na plnění předmětu veřejné zakázky podílet například v rozsahu, který odpovídá za Dodavatele prokazovanou kvalifikací. Jedná se o tyto činnosti realizované typy:

- Specialista architekt řešení
IT specialista na bezpečnostní technologie – LAN- 1
IT specialista na bezpečnostní technologie – LAN- 2
IT specialista pro systémy LAN SDN - 1
IT specialista pro systémy LAN SDN - 2
IT specialista na serverové virtualizace - 2

Podávatel se tímto nadávatelem a nepodávatelem ve vztahu k čl. 81 odst. 2 zákona č. 134/2016 Sb., o způsobech výběru veřejných zakázek, závazuje se své společnosti a osobám odpovědným za plnění veřejné zakázky společně s Dodavatelem a dle ustanovení a odlišností Dodavatele ze vztahu ústředí, náklady, služby, konzultace nebo jiné služby (včetně, náklady však výjimečně, částky ústředí a náklady na základě souhlasu dodavatele, ústředí a náklady na práci zastupující nebo jiných služeb a vztahů vyhovující nebo obhajoby vůči nákladům nebo tvůrčími službami jinými povahy, které Dodavatel vztahuje, přičemž z toho vzniklé v souvislosti s poskytováním činností Podávatele nebo v rozporu s ním.

V Praze, dne 29. 6. 2018

ALEFNULA, a.s.
Pernerova 69/42, 186 00 Praha 8
IČ: 61858579 DIČ: CZ61858579

ALEF NULA, a.s.
[redacted] Sdělit Director
za Podávatele

Písemný závazek: Podávatel vztahuje v rozsahu požadovaném výše akceptuje.

V Praze, dne: 27.6.2018



Corpus Solutions a.s.
Sokolova 1636/18
140 00 Praha 4
IČ: 25764616

Corpus Solutions a.s.
[redacted] předseda představenstva
za Dodavatele

Plná moc

Název: ALEF NULA, a.s.
Zastupující / jednající: [redacted] předseda představenstva
IČ: 61858579

limto zmocňuje

Jméno: [redacted]
Bytem: [redacted]
Datum naryzení: [redacted]
Funkce v organizaci / značení: [redacted]
Umožnění:

Číslo a obsah: [redacted]

Handwritten note: "Všechny souhlasím, neproblemy poskytnout sítě"
"provozovat" "zadání, které Hlavou máte před."

V Praze dne 29. 6. 2018

V Praze dne 29. 6. 2018

Tato plná moc platí do: 30. 6. 2018

ALEFNULA, a.s.
Pernerova 69/42, 186 00 Praha 8
IČ: 61858579

ALEF NULA, a.s.
Pernerova 69/42, 186 00 Praha 8
IČ: 61858579

5.2 Osvědčení o způsobilosti dle vyhlášky č. 50/1978 Sb.

145 84-0022

OSVĚDČENÍ

[Redacted] se. Jiří, Vít a Lubomír
Emanuela Dvořák, Dvořák a kolektiv
Corpus Solutions a.s.
Hradec, nabývání

3. 6. 2018, 10:00

145 84-0022



6 Informace o celkovém počtu listů nabídky

Čestné prohlášení

o počtu stran

Uchazeč, společnost Corpus Solutions a. s., se sídlem Štětkova 1638/18, 140 00 Praha 4, IČ:25764616 tímto prohlašuje, že:

- židovaných listů je 190
- celkový počet listů je 190

V Praze dne 27. 06. 2018



Člen představenstva
Corpus Solutions a.s.

