

RÁMCOVÁ SMLOUVA NA DODÁVKU AKTIVNÍCH PRVKŮ A ROZŠIŘUJÍCÍCH MODULŮ

Smluvní strany:

Česká republika – Česká správa sociálního zabezpečení

se sídlem: Křížová 25, 225 08 Praha 5

IČO: 00006963

DIČ: neplátce

bankovní spojení: Česká národní banka, číslo účtu: 10006-127001/0710

ID datové schránky: 49kaiq3

statutární zástupce: Mgr. František Boháček, ústřední ředitel

zastoupená: **Ing. Milanem Shrbeným**, ředitelem sekce informačních a komunikačních technologií

(dále jen „**Objednatel**“)

a

ELSO PHILIPS SERVICE spol. s r.o.

se sídlem: Kladenská 1879/3, 160 00 Praha 6

IČO: 48113336

DIČ: CZ48113336

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 16471

bankovní spojení: ČSOB a.s., číslo účtu: 800240993/0300

ID datové schránky: 8443xnv

zastoupená: [REDACTED] jednatelem

(dále jen „**Poskytovatel**“)

dnešního dne uzavřely tuto smlouvu v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „**občanský zákoník**“) (dále jen „**Smlouva**“)

Smluvní strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:

1. ÚVODNÍ UJEDNÁNÍ

- 1.1 Objednatel prohlašuje, že:
- 1.1.1 je organizační složkou České republiky;
 - 1.1.2 je správcem a provozovatelem Integrovaného informačního systému ČSSZ (dále jen „**IIS ČSSZ**“), který je podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, informačním systémem státní správy;
 - 1.1.3 IIS ČSSZ je prvkem kritické informační infrastruktury podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „**zákon o kybernetické bezpečnosti**“);
 - 1.1.4 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.
- 1.2 Poskytovatel prohlašuje, že:
- 1.2.1 je podnikatelem dle ustanovení § 420 a násl. občanského zákoníku;
 - 1.2.2 ke dni uzavření této Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat;
 - 1.2.3 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.
- 1.3 Objednatel oznámil dne 9.10.2020 oznámením otevřeného řízení svůj záměr zadat veřejnou zakázku s názvem „*Rámcová smlouva na dodávku aktivních prvků a rozšiřujících modulů*“, ev. č. Z2020-035467 (dále jen „**Veřejná zakázka**“) dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „**ZZVZ**“). Na základě tohoto zadávacího řízení byla pro plnění Veřejné zakázky vybrána nabídka Poskytovatele v souladu s ustanovením § 122 odst. 1 ZZVZ.

2. ÚČEL SMLOUVY

- 2.1 Účelem této Smlouvy je zajištění realizace Veřejné zakázky dle zadávací dokumentace Veřejné zakázky (dále jen „**Zadávací dokumentace**“), tedy zajištění podmínek pro obnovu, údržbu a rozvoj stávající síťové infrastruktury Objednatele, a to v souladu s požadavky Objednatele definovanými touto Smlouvou.

- 2.2 Poskytovatel touto Smlouvou garantuje Objednateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle Zadávací dokumentace. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:
- 2.2.1 v případě jakékoliv nejistoty ohledně výkladu ujednání této Smlouvy budou tato ujednání vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený Zadávací dokumentací;
 - 2.2.2 v případě chybějících ujednání této Smlouvy budou použita dostatečně konkrétní ujednání Zadávací dokumentace;
 - 2.2.3 Poskytovatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

3. PŘEDMĚT SMLOUVY

- 3.1 Předmětem této Smlouvy je rámcový závazek Poskytovatele dodávat Objednateli prostřednictvím jednotlivých dílčích veřejných zakázek (dílčích smluv) plnění spočívající v dodávce (poskytnutí):
- 3.1.1 aktivních prvků (hardware), včetně poskytnutí licencí k softwaru, který tvoří příslušenství aktivních prvků,
 - 3.1.2 rozšiřujících modulů (hardware),
- (aktivní prvky a rozšiřující moduly společně dále jen jako „**Zařízení**“)
- 3.1.3 školení,
- a to vše dle specifikace uvedené v Příloze č. 1 a Příloze č. 2 této Smlouvy (dále společně jen „**Plnění**“).
- 3.2 Součástí Plnění je také zajištění podpory Zařízení, včetně software, ze strany jeho výrobce v délce 36 měsíců ode dne převzetí příslušného hardware v rámci Plnění, tedy ode dne podpisu příslušného předávacího protokolu (dále jen „**Podpora**“). Rozsah Podpory je uveden na webových stránkách výrobce Zařízení <https://software.cisco.com/>.
- 3.3 Plnění bude poskytováno vždy na základě dílčích smluv uzavíraných postupem specifikovaným v čl. 4. této Smlouvy (dále jen „**Dílčí smlouva**“). Vzor Dílčí smlouvy je uveden v Příloze č. 7 této Smlouvy
- 3.4 Objednatel poskytne Poskytovateli nezbytnou součinnost při poskytování Plnění.
- 3.5 Objednatel převezme Plnění a zaplatí Poskytovateli dohodnutou cenu za řádně a včas poskytnuté Plnění za podmínek dále stanovených touto Smlouvou a Dílčí smlouvou.
- 3.6 Objednatel nemusí po dobu trvání této Smlouvy požadovat ani jedno Plnění.
- 3.7 Poskytovatel bude pro Objednatele poskytovat školení prostřednictvím členů realizačního týmu uvedených v Příloze č. 6 této Smlouvy. Změna členů realizačního týmu je možná pouze na základě předchozího písemného souhlasu Objednatele s takovou změnou. Tento souhlas Objednatel neodepře, pokud v případě změny v obsazení realizačního týmu budou veškeré osoby nadále splňovat kvalifikační požadavky Objednatele na tyto osoby vyjádřené v Zadávací dokumentaci.

- 3.8 Specifikace jednotlivých školení je uvedena v Příloze č. 2 této Smlouvy. Podrobnosti konání jednotlivých požadovaných školení, zejména termín a místo konání, časová náročnost a počet zaměstnanců Objednatele, kteří se školení budou účastnit, budou dopředu mezi smluvními stranami vždy domluveny. Každého školení se zúčastní současně maximálně 6 zaměstnanců Objednatele.
- 3.9 Poskytovatel bude poskytovat Plnění sám nebo s využitím poddodavatelů uvedených v Příloze č. 4 této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena Objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval Poskytovatel sám. Smluvní strany výslovně uvádějí, že při poskytování Plnění prostřednictvím jakékoliv třetí osoby dle tohoto odstavce má Poskytovatel odpovědnost, jako by poskytování Plnění realizoval sám.
- 3.10 Poskytovatel v rámci Plnění převede na Objednatele vlastnické právo k Zařízení a předá mu veškeré doklady, které jsou nutné k převzetí a řádnému užívání Zařízení, včetně potvrzení výrobce (anebo jeho oficiálního zastoupení pro území České republiky), že veškerá dodaná Zařízení jsou nová.
- 3.11 V případě, že v zadávacím řízení Veřejné zakázky podával Poskytovatel společnou nabídku, nesou všechny subjekty na straně Poskytovatele uvedené na úvodní straně této Smlouvy odpovědnost z plnění z této Smlouvy společně a nerozdílně.

4. UZAVÍRÁNÍ DÍLČÍCH SMLUV

- 4.1 Dílčí smlouva je uzavřena na základě písemné výzvy k poskytnutí plnění, jež je návrhem na uzavření Dílčí smlouvy (dále jen „**Výzva**“), a jejím přijetím a potvrzením Poskytovatelem. Výzva musí být učiněna v elektronické podobě.
- 4.2 Poskytovatel je povinen Výzvu Objednatele potvrdit nejpozději do 10 pracovních dnů ode dne jejího doručení Poskytovateli, s výjimkou případů, kdy (i) Poskytovatel oznámí Objednateli nezbytnost prodloužení této lhůty, a to zejména s ohledem na objektivní složitost požadovaného předmětu dílčího plnění; (ii) Poskytovateli brání v potvrzení Výzvy vážné důvody, které není schopen objektivně překonat, přičemž je Poskytovatel povinen tyto důvody Objednateli neprodleně oznámit.
- 4.3 Výzva musí obsahovat zejména následující náležitosti:
- 4.3.1 označení této Smlouvy a smluvních stran a pořadové číslo dle vzestupného číslování od počátku plnění dle této Smlouvy;
 - 4.3.2 druh a počet požadovaného Plnění;
 - 4.3.3 požadovaný termín poskytnutí Plnění;
 - 4.3.4 cenu Plnění dle Přílohy č. 5 této Smlouvy;
 - 4.3.5 specifikaci místa plnění; a
 - 4.3.6 podpis osoby oprávněné zastupovat Objednatele.
- 4.4 V případě, že Výzva neobsahuje všechny povinné náležitosti uvedené v odst. 4.3 tohoto článku této Smlouvy nebo obsahuje vady, je Poskytovatel oprávněn Výzvu odmítnout, je však povinen o tom Objednatele písemně informovat, včetně označení těch částí Výzvy, které jsou v rozporu s odst. 4.3 tohoto článku této Smlouvy, a to nejpozději ve lhůtě 5 pracovních dnů od jejího doručení. Vadou Výzvy je zejména

neurčitost zadání nebo rozpor s touto Smlouvou. Vadou Výzvy také je, pokud obsahuje nepřiměřeně krátký termín plnění. Objednatel je povinen odstranit případné vady Výzvy, které budou řádně specifikované Poskytovatelem, a Výzvu opětovně předložit Poskytovateli. Neodstraní-li Objednatel vady Výzvy, je Poskytovatel povinen průběžně (minimálně 1x měsíčně) na trvání tohoto stavu Objednatele upozorňovat, a to až do té doby, než Objednatel rozhodne, že Výzvu bere zpět, nebo specifikované vady odstraní.

- 4.5 V případě že Výzva neobsahuje vady dle odst. 4.4 tohoto článku této Smlouvy, zavazuje se Poskytovatel tuto Výzvu bez zbytečného odkladu, nejpozději však do 5 pracovních dnů od jejího doručení, písemně potvrdit a uzavřít tak Dílčí smlouvu.
- 4.6 V případě, že Výzva nebude ve lhůtě dle odst. 4.5 tohoto článku této Smlouvy Poskytovatelem přijata a současně pokud Poskytovatel nevznese písemné připomínky k Výzvě ve smyslu odst. 4.4 tohoto článku této Smlouvy, považuje se Dílčí smlouva uplynutím této lhůty za schválenou.
- 4.7 Objednatel není povinen po dobu účinnosti této Smlouvy uskutečnit ani jednu Výzvu.

5. DOBA A MÍSTO PLNĚNÍ

- 5.1 Poskytovatel je povinen poskytnout Plnění vždy nejpozději do 8 týdnů ode dne nabytí účinnosti příslušné Dílčí smlouvy, nebylo-li v Dílčí smlouvě stanoveno jinak.
- 5.2 Místem plnění je sídlo Objednatele a dále budova Objednatele na adrese Trojská 1997/13a, 182 00 Praha 8. Objednatel specifikuje místo plnění v Dílčí smlouvě, resp. ve Výzvě.
- 5.3 Pokud to povaha Plnění umožňuje a Objednatel vůči tomu nemá výhrady, je Poskytovatel oprávněn provádět příslušné části Plnění vzdáleným přístupem.

6. KVALITATIVNÍ POŽADAVKY NA PLNĚNÍ

- 6.1 Poskytovatel dodá Objednateli Zařízení, která budou:
 - 6.1.1 nová a nepoužitá;
 - 6.1.2 plně funkční;
 - 6.1.3 použitelná Objednatelem v České republice. Zejména v této souvislosti Poskytovatel zaručuje Objednateli, že Zařízení získala veškerá nezbytná osvědčení pro užití v České republice, a to jak z pohledu obecně závazných právních předpisů, tak podmínek výrobce pro poskytování Podpory. Poskytovatel předá kopie těchto osvědčení Objednateli při předání Zařízení;
 - 6.1.4 mít jakost a provedení stanovené v této Smlouvě, případně v Dílčí smlouvě;
 - 6.1.5 bez materiálových, konstrukčních, výrobních a vzhledových či jiných vad;
 - 6.1.6 splňovat veškeré nároky a požadavky českého právního řádu, zejména zákona č. 185/2001 Sb., o odpadech a o změně některých dalších zákonů a zákona č. 477/2001 Sb., o obalech a o změně některých zákonů (zákon o obalech);
 - 6.1.7 dodána včetně všech souvisejících licencí specifikovaných v Příloze č. 1 této Smlouvy a jiných systémových licencí nezbytných k řádnému užívání Zařízení;

- 6.1.8 bezpečná v tom smyslu, že dodávky nebudou obsahovat radioaktivní materiály a jiné nebezpečné látky a věci, které se mohou stát nebezpečným odpadem ve smyslu zákona č. 185/2001 Sb., o odpadech a o změně některých dalších zákonů;
- 6.1.9 ve vlastnictví Poskytovatele, který je bez dalšího vlastnické právo oprávněn na Objednatele převést; a
- 6.1.10 nezatížena zástavními, předkupními, nájemními či jinými právy třetích osob.
- 6.2 Poskytovatel zaručuje Objednateli, že veškerý software bude plně funkční a způsobilý pro použití k určenému účelu, pro užití v České republice, bude odpovídat sjednané specifikaci, bude bez faktických i právních vad, a bude splňovat veškeré nároky a požadavky českého právního řádu a Objednatele.
- 6.3 Poskytovatel uhradí veškeré případné daně a poplatky týkající se softwaru, které nejsou zahrnuty v ceně Plnění.
- 6.4 Po dobu trvání záruční doby a po dobu trvání Podpory musí Poskytovatel:
 - 6.4.1 mít uzavřenou dohodu o podpoře s výrobcem Zařízení na všechna dodaná Zařízení tak, aby v případě závady na dodaném Zařízení, kterou není Poskytovatel schopen sám odstranit, bylo možné eskalovat závadu přímo k výrobcí Zařízení nebo jím pověřenému servisnímu partnerovi;
 - 6.4.2 zajistit Objednateli přístup k dokumentaci výrobce Zařízení a znalostní bázi výrobce Zařízení, kterou výrobce Zařízení poskytuje v rámci Podpory;
 - 6.4.3 poskytnout Objednateli všechny relevantní software releases a verze software nabízené výrobcem software tak, aby dodané řešení vyhovovalo zadání Objednatele a fungovalo bez závad;
 - 6.4.4 informovat Objednatele o nových verzích a funkcích software, které mohou rozšiřovat dodané řešení způsobem, který Objednatel shledá ve shodě s jeho potřebami dalšího rozvoje dodaného řešení;
 - 6.4.5 zajistit službu hlášení chyb software, které jsou oznámeny výrobcem; a
 - 6.4.6 umožnit eskalaci závad k výrobcí software.
- 6.5 Poskytovatel doloží Objednateli potvrzení, že Podpora výrobce je určena pro koncového zákazníka pro využití na území České republiky, ke dni nabytí účinnosti této Smlouvy.
- 6.6 Poskytovatel zajistí dostupnost náhradních dílů od výrobce Zařízení a dostupnost Podpory pro dodané řešení.
- 6.7 Poskytovatel zajistí technickou podporu výrobce Zařízení v režimu 24x7x365.
- 6.8 Poskytovatel zajistí výměnu vadného Zařízení za nové s garantovanou dobou opravy 8x5 NBD (Next Business Day).
- 6.9 Veškeré závady budou Objednatelem hlášeny prostřednictvím jeho ServiceDesku, pouze v případě nefunkčnosti ServiceDesku budou závady Objednatelem hlášeny prostřednictvím e-mailu na e-mailovou adresu [REDACTED] Oznámení závady bude obsahovat zejména popis závady, popř. jejího projevu, není-li možné, aby Objednatel popsal samotnou podstatu závady.

- 6.10 Za vyřešení závady se považuje okamžik přijetí zprávy o vyřešení závady v systému ServiceDesk Objednatele či přijetí e-mailu od Poskytovatele o odstranění závady Objednatelem.
- 6.11 Poskytovatel přizpůsobí svůj ServiceDesk stavu ServiceDesku Objednatele a zajistí takové propojení, které zaručí bezproblémovou komunikaci ServiceDesků navzájem, a to vše do 10 pracovních dnů ode dne nabytí účinnosti této Smlouvy.
- 6.12 Plnění bude poskytováno v souladu se standardy Objednatele, jejichž soupis je uveden v Příloze č. 8 této Smlouvy. Objednatel se zavazuje Poskytovateli předat dokumentaci se standardy Objednatele, jejichž soupis je uveden v Příloze č. 8 této Smlouvy a průběžně jej seznamovat s jejich platnou verzí.

7. POTVRZENÍ O POSKYTNUTÍ PLNĚNÍ (AKCEPTACE)

- 7.1 Potvrzení o poskytnutí Plnění (akceptace) bude provedeno prostřednictvím písemného předávacího protokolu.
- 7.2 Školení bude akceptováno podpisem protokolu o absolvování školení ze strany Objednatele.
- 7.3 Objednatel nabývá vlastnické právo k Zařízením okamžikem akceptace Plnění, tj. okamžikem podpisu předávacího protokolu Objednatelem.
- 7.4 Nebezpečí škody na Zařízeních přechází z Poskytovatele na Objednatele okamžikem akceptace Plnění, tj. okamžikem podpisu předávacího (akceptačního) protokolu Objednatelem.
- 7.5 Dodaná Zařízení, včetně software, je Poskytovatel povinen při odeslání k přepravě k Objednateli řádně zabalit takovým způsobem, aby při prováděné přepravě nedošlo k jejich znehodnocení či k jakémukoliv jeho poškození. Poskytovatel je povinen zajistit likvidaci a odvoz všech obalových materiálů v rámci Plnění.

8. CENA A PLATEBNÍ PODMÍNKY

- 8.1 Cena za Plnění poskytnuté na základě Dílčí smlouvy bude stanovena v souladu s jednotkovými cenami za příslušné Plnění uvedenými v Příloze č. 5 této Smlouvy.
- 8.2 Ceny uvedené v Příloze č. 5 této Smlouvy jsou stanoveny jako maximální a nepřekročitelné a nejvýše tyto částky je Poskytovatel oprávněn Objednateli účtovat. Ceny uvedené v Příloze č. 5 této Smlouvy mohou být překročeny pouze v souvislosti se změnou sazby DPH mající prokazatelný vliv na tyto ceny, a to pouze o výši, která této změně bude odpovídat. Z jakýchkoliv jiných důvodů nesmí být ceny uvedené v Příloze č. 5 této Smlouvy překročeny.
- 8.3 Poskytovatel výslovně prohlašuje, že cena za poskytnutí Plnění dle Dílčí smlouvy již v sobě bude zahrnovat veškeré náklady Poskytovatele spojené s tímto plněním. Cena za poskytnutí Plnění dle konkrétní Dílčí smlouvy bude cenou konečnou, nejvýše přípustnou a nemůže být změněna.
- 8.4 Cena za poskytnutí Plnění bude Objednatelem Poskytovateli hrazena na základě daňového dokladu (faktury). Poskytovatel předloží Objednateli daňový doklad (fakturu) až po řádném potvrzení poskytnutí Plnění (akceptaci) Objednatelem.

Objednatel potvrdí předávací protokol nebo protokol o absolvování školení, případně kopie těchto dokumentů, bude nedílnou součástí příslušného daňového dokladu (faktury).

- 8.5 Splatnost jednotlivých daňových dokladů (faktur) se sjednává na 30 dnů ode dne jejich doručení povinné smluvní straně. Toto ujednání se uplatní i v případě hrazení smluvních pokut.
- 8.6 Každý daňový doklad (faktura) musí obsahovat náležitosti daňového dokladu dle platných a účinných právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dle této Smlouvy. V případě, že daňový doklad (faktura) nebude mít odpovídající náležitosti, je Objednatel oprávněn daňový doklad (fakturu) zaslat ve lhůtě splatnosti zpět Poskytovateli k doplnění či opravě, aniž se tak dostane do prodlení s úhradou oprávněně fakturované ceny; lhůta splatnosti počíná běžet znovu ode dne doručení náležitě doplněného či opraveného daňového dokladu (faktury) Objednateli.
- 8.7 Platby peněžitých částek se provádí bankovním převodem na účet druhé smluvní strany uvedený v daňovém dokladu (faktuře).
- 8.8 Objednatel neposkytuje Poskytovateli na poskytování Plnění jakékoliv zálohy.
- 8.9 Veškeré platby budou probíhat výhradně v české měně (CZK) a rovněž veškeré cenové údaje budou uvedeny v této měně.
- 8.10 Objednatel bude hradit přijaté daňové doklady (faktury) pouze na bankovní účty Poskytovatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 96 odst. 2 zákona o DPH. V případě, že Poskytovatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí Objednatel Poskytovateli pouze základ daně, přičemž DPH uhradí Poskytovateli až po zveřejnění příslušného účtu Poskytovatele v registru plátců a identifikovaných osob Poskytovatelem.
- 8.11 Poskytovatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Poskytovatel je nespolehlivým plátcem ve smyslu ustanovení § 106a zákona o DPH (dále jen „**nespolehlivý plátcem**“). V případě, že správce daně rozhodne o tom, že Poskytovatel je nespolehlivým plátcem, zavazuje se Poskytovatel o tomto informovat Objednatele do dvou pracovních dnů. Stane-li se Poskytovatel nespolehlivým plátcem, uhradí Objednatel Poskytovateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Poskytovateli až po písemném doložení Poskytovatele o jeho úhradě této DPH příslušnému správci daně.

9. PRÁVA A POVINNOSTI POSKYTOVATELE, SOUČINNOST OBJEDNATELE

- 9.1 Poskytovatel v rámci poskytování Plnění:
 - 9.1.1 bude poskytovat Plnění vlastním jménem, na vlastní odpovědnost a v souladu s pokyny Objednatele řádně a včas a s péčí řádného hospodáře, v souladu s podmínkami sjednanými v této Smlouvě a s procesy „best practice“;
 - 9.1.2 zabalí předmět Plnění či jinak opatří pro přepravu způsobem zabraňujícím jeho poškození nebo znehodnocení;
 - 9.1.3 předloží Objednateli na jeho žádost, nejpozději do tří pracovních dnů ode dne jejího obdržení, písemné potvrzení zastoupení výrobce o určení Zařízení pro trh v České republice a pro Objednatele jako koncového zákazníka, je-li

- registrace koncového zákazníka nezbytná k řádnému užívání Zařízení (včetně seznamu sériových čísel dodávaných Zařízení);
- 9.1.4 upozorní Objednatele na všechny hrozící vady Plnění či potenciální výpadky Plnění, jakož i poskytne Objednateli veškeré informace, které jsou pro poskytování Plnění nezbytné,
- 9.1.5 neprodleně oznámí Objednateli jakékoli překážky, které mu brání v poskytování Plnění a výkonu dalších činností souvisejících s Plněním,
- 9.1.6 upozorní Objednatele na potenciální rizika vzniku škod a provede včas a řádně na své náklady taková opatření, která riziko sníží nebo zcela vyloučí,
- 9.1.7 upozorní Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele;
- 9.1.8 i bez pokynů Objednatele provede nutné úkony, které ač nejsou předmětem této Smlouvy, budou s ohledem na nepředvídatelné okolnosti pro poskytování Plnění nezbytné nebo jsou nezbytné pro zamezení vzniku škody,
- 9.1.9 bude dodržovat bezpečnostní, hygienické, požární, organizační a ekologické právní předpisy a vnitřní předpisy Objednatele, se kterými byl prokazatelně seznámen nebo které jsou všeobecně známé,
- 9.1.10 bude řešit písemné požadavky či dotazy Objednatele vztahující se k Plnění, a to nejpozději ve lhůtě 5 pracovních dnů ode dne jejich doručení Poskytovateli.
- 9.2 Objednatel poskytne Poskytovateli ke splnění závazků dle této Smlouvy nezbytně nutnou součinnost, zejména bude včas informovat Poskytovatele o všech organizačních změnách, poznatcích z kontrolní činnosti a dalších skutečnostech významných pro poskytování Plnění.
- 9.3 V rámci součinnosti Objednatel umožní Poskytovateli užití vybraných hardwarových a softwarových prostředků Objednatele, a to výhradně za účelem poskytování Plnění a pouze po dobu účinnosti této Smlouvy, resp. Dílčích smluv. Poskytovatel bude užívat tyto prostředky řádně a v souladu s provozními a bezpečnostními postupy či pokyny Objednatele. Poskytovatel nesmí a nebude s těmito prostředky Objednatele nakládat nebo je používat v rozporu s touto Smlouvou.
- 9.4 Poskytovatel bude udržovat v platnosti a účinnosti po celou dobu účinnosti této Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě (zejména Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy, nesmí být nižší než 50.000.000,- Kč za rok a to se spoluúčastí max. 10 %. Pojistnou smlouvu dle tohoto odstavce, pojistku potvrzující uzavření takové smlouvy nebo pojistný certifikát potvrzující uzavření takové smlouvy je Poskytovatel povinen předložit Objednateli kdykoliv po písemném vyžádání Objednatele, a to do 5 pracovních dnů. Nepředložením pojistné smlouvy, pojistky nebo pojistného certifikátu ve výše uvedených lhůtách vzniká právo Objednatele na odstoupení od této Smlouvy.
- 9.5 Poskytovatel neprodleně informuje Objednatele o významné změně kontroly nad Poskytovatelem podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, nebo změny nad zásadními aktivy využívanými Poskytovatelem k plnění podle této Smlouvy.

10. ZÁRUKA ZA JAKOST

- 10.1 Poskytovatel poskytuje záruku, že každé Zařízení má ke dni akceptace funkční vlastnosti stanovené touto Smlouvou a je způsobilé k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.
- 10.2 Poskytovatel poskytuje záruku za jakost každého Zařízení od okamžiku jeho akceptace po dobu 36 měsíců.
- 10.3 Objednatel je oprávněn vady Zařízení nahlásit Poskytovateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena. Nahlašování záručních vad probíhá primárně prostřednictvím ServiceDesku Objednatele, případně prostřednictvím datové schránky.
- 10.4 Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.
- 10.5 Zařízení má vady, zejména pokud nebylo poskytnuto v sjednaném druhu, množství a jakosti. Za vady Zařízení se považují i vady v návodech (manuálech) k použití, dokladech a dokumentech.
- 10.6 V případě, že je dodáno Zařízení s vadami, či se na Zařízení vady v záruční době vyskytnou, je Poskytovatel povinen vady odstranit opravou, dodáním náhradního zboží, či přiměřenou slevou z ceny, a to dle volby Objednatele.
- 10.7 Poskytovatel odstraní vady Zařízení nebo dodá nové Zařízení do 3 pracovních dnů ode dne, kdy mu byly vady dle předchozího odstavce oznámeny. Nové Zařízení musí splňovat veškeré požadavky kladené na Zařízení dodávaná na základě této Smlouvy.
- 10.8 V případě odstranění závady dodáním nového Zařízení poskytuje Poskytovatel na takové Zařízení záruku za jakost v délce trvání 36 kalendářních měsíců.
- 10.9 Pokud Poskytovatel neodstraní závadu krytou zárukou za jakost řádně ve stanovené lhůtě, může Objednatel nechat závadu odstranit třetí osobou a Poskytovatel uhradí bez zbytečného odkladu Objednateli účelně vynaložené náklady v souvislosti s odstraněním závady.
- 10.10 Nároky z vad se nedotýkají nároku Objednatele, na náhradu škody nebo na smluvní pokutu.

11. UŽÍVACÍ PRÁVA K SOFTWARE

- 11.1 Vzhledem k tomu, že součástí Plnění dle této Smlouvy je i software, který ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) (dále jen „**autorský zákon**“), může naplňovat znaky autorského díla či být považován za autorské dílo ve smyslu autorského zákona (dále společně jen „**autorské dílo**“), je k tomuto plnění poskytována či postupována licence či podlicence (dále společně jen „**licence**“) za podmínek sjednaných dále v tomto článku této Smlouvy.
- 11.2 Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k autorskému dílu užívat toto autorské dílo v následujícím rozsahu: udělená licence zahrnuje nevýhradní oprávnění užít autorské dílo v rozsahu, v jakém je to nezbytné pro řádné fungování aktivních prvků (hardware), a to po dobu užívání těchto aktivních prvků (hardware) Objednatelem, nejdéle však po dobu 10 let od akceptace předmětné části Plnění, na

území České republiky a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Objednatele.

- 11.3 Licence k autorskému dílu je poskytována jako nevýhradní. Objednatel není povinen licenci využít.
- 11.4 Účinnost licence nastává okamžikem akceptace Plnění, které příslušné autorské dílo obsahuje; do té doby je Objednatel oprávněn autorské dílo užit v rozsahu a způsobem nezbytným k provedení akceptace příslušného Plnění.
- 11.5 Udělení licence nelze ze strany Poskytovatele vypovědět a její účinnost trvá i po skončení účinnosti této Smlouvy, nedohodnou-li se smluvní strany výslovně jinak.
- 11.6 Pro vyloučení veškerých pochybností smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle této Smlouvy vznikne činností Poskytovatele a Objednatele dílo spoluautorů a nedohodnou-li se smluvní strany výslovně jinak, platí, že k okamžiku vzniku takového díla spoluautorů postoupil Poskytovatel Objednateli právo vykonávat majetková autorská práva k dílu spoluautorů a udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena Plnění je stanovena se zohledněním tohoto ujednání a Poskytovateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.
- 11.7 Poskytovatel je povinen postupovat tak, aby udělení licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.
- 11.8 Objednateli nemusí být k softwaru předány zdrojové kódy a stejně tak nemusí být Objednateli poskytnuto právo do standardního softwaru zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace. Součástí licence je též právo k provedeným změnám konfigurace či nastavením počítačových programů.
- 11.9 Jestliže jsou s užitím software spojeny jednorázové či pravidelné poplatky, je Poskytovatel povinen v rámci ceny Plnění řádně uhradit všechny tyto poplatky za dobu 36 měsíců od akceptace předmětné části Plnění.
- 11.10 Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Poskytovatelem Objednateli.
- 11.11 Odměna za poskytnutí licence k autorským dílům je zahrnuta v ceně Plnění dle této Smlouvy. Bez ohledu na formu uzavření licenční smlouvy však platí, že Poskytovatel je vždy povinen zajistit poskytnutí licence dle podmínek stanovených touto Smlouvou, a to bez ohledu na případný rozdílný obsah standardních licenčních podmínek vykonavatele majetkových práv k takovým autorským dílům.

12. OPRAVNĚNÉ OSOBY

- 12.1 Každá ze smluvních stran jmenuje oprávněnou osobu. Oprávněné osoby budou zastupovat smluvní stranu ve smluvních, obchodních, a technických záležitostech souvisejících s plněním této Smlouvy a ve věcech kybernetických bezpečnostních událostí a incidentů souvisejících s touto Smlouvou. Pro vyloučení pochybností se smluvní strany dohodly, že:

- 12.1.1 osoby oprávněné jednat v záležitostech smluvních jsou oprávněny vést s druhou smluvní stranou jednání obchodního charakteru, podepisovat Výzvu, uzavírat Dílčí smlouvy a měnit či rušit tuto Smlouvu či Dílčí smlouvu a uzavírat k nim dodatky;
- 12.1.2 osoby oprávněné v záležitostech obchodních jsou oprávněny vést s druhou stranou jednání obchodního charakteru, jednat o Dílčích smlouvách, jednat v rámci akceptačních procedur při předávání a převzetí Plnění, zejména podepisovat příslušné akceptační, předávací či jiné protokoly dle této Smlouvy; osoby oprávněné v záležitostech obchodních však nejsou oprávněny tuto Smlouvu či Dílčí smlouvu měnit či rušit ani k nim uzavírat dodatky;
- 12.1.3 osoby oprávněné jednat v záležitostech technických jsou oprávněny vést jednání technického charakteru, poskytovat stanoviska v technických otázkách a jednat jménem stran v rámci reklamace vad a při uplatňování záruky; tyto osoby rovněž nejsou oprávněny tuto Smlouvu či Dílčí smlouvu měnit či rušit ani k nim uzavírat dodatky;
- 12.1.4 osoby oprávněné jednat ve věcech kybernetických bezpečnostních událostí a incidentů souvisejících s touto Smlouvou jsou oprávněny vést jednání týkající se kybernetických bezpečnostních incidentů souvisejících s plněním předmětu této Smlouvy.
- 12.2 Jména oprávněných osob jsou uvedena v Příloze č. 3 této Smlouvy.
- 12.3 Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny na takovou změnu druhou smluvní stranu písemně upozornit. O takovéto změně nebude uzavírán dodatek k této Smlouvě. Změna je účinná ode dne doručení písemného upozornění o změně oprávněné osoby druhé smluvní straně.
- 12.4 Poskytovatel se zavazuje ve lhůtě 5 pracovních dnů ode dne doručení odůvodněné písemné žádosti Objednatele o výměnu oprávněné osoby Poskytovatele podílející se na plnění této Smlouvy, s níž Objednatel nebyl z jakéhokoliv důvodu spokojen, nahradit jinou vhodnou osobou s odpovídající kvalifikací.

13. OCHRANA INFORMACÍ A OSOBNÍCH ÚDAJŮ

- 13.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy, resp. z Dílčích smluv:
 - 13.1.1 si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**“),
 - 13.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.
- 13.2 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této Smlouvy, resp. Dílčí smlouvy, získala od druhé smluvní strany.
- 13.3 Za třetí osoby se nepovažují:
 - 13.3.1 zaměstnanci smluvních stran a osoby v obdobném postavení,

13.3.2 orgány smluvních stran a jejich členové,

13.3.3 ve vztahu k důvěrným informacím Objednatele poddodavatelé Poskytovatele,

13.3.4 ve vztahu k důvěrným informacím Poskytovatele externí dodavatelé Objednatele, a to i potenciální,

za předpokladu, že se podílejí na plnění této Smlouvy, resp. Dílčí smlouvy nebo na plnění spojeném s plněním dle této Smlouvy, resp. Dílčí smlouvy, důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvními stranám v této Smlouvě.

- 13.4 Veškeré informace poskytnuté Objednatelem Poskytovateli se považují za důvěrné, není-li stanoveno jinak. Veškeré informace poskytnuté Poskytovatelem Objednatelem se považují za důvěrné, pouze pokud na jejich důvěrnost Poskytovatel Objednatele předem písemně upozornil a Objednatel Poskytovateli písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat. Pokud jsou důvěrné informace Poskytovatele poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je Poskytovatel povinen upozornit Objednatele na důvěrnost takového materiálu též jejím vyznačením alespoň na titulní stránce nebo přední straně média.
- 13.5 Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit důvěrné informace vyplývající z této Smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající z právních předpisů upravujících ochranu osobních údajů. Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této Smlouvy, resp. Dílčí smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podléajícími se na plnění této Smlouvy, resp. Dílčí smlouvy.
- 13.6 Budou-li informace poskytnuté Objednatelem či třetími stranami, které jsou nezbytné pro plnění dle této Smlouvy, resp. Dílčí smlouvy, obsahovat osobní údaje, zavazuje se Poskytovatel zabezpečit splnění všech ohlašovacích povinností, které příslušný zákon vyžaduje a které mohou být dle právních předpisů upravujících ochranu osobních údajů splněny zpracovatelem osobních údajů, a obstarat předepsané souhlasy subjektů osobních údajů předaných ke zpracování, pokud jsou takové souhlasy dle právních předpisů upravujících ochranu osobních údajů v konkrétním případě vyžadovány.
- 13.7 Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, resp. Dílčí smlouvy, se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu, resp. Dílčí smlouvy. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé smluvní strany jinak, než za účelem plnění této Smlouvy, resp. Dílčí smlouvy.
- 13.8 Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je předávající strana

povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce nebo přední straně média. Absence takového upozornění však nezpůsobuje zánik povinnosti ochrany takto poskytnutých informací.

- 13.9 Bez ohledu na výše uvedená ujednání se za důvěrné nepovažují informace, které:
- 13.9.1 se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající smluvní strany či právních předpisů,
 - 13.9.2 měla přijímající strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
 - 13.9.3 jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
 - 13.9.4 po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi,
 - 13.9.5 vyžaduje zákon či jiný právní předpis včetně práva EU nebo závazné rozhodnutí oprávněného orgánu veřejné moci zpřístupnit,
 - 13.9.6 jsou obsažené ve Smlouvě, resp. Dílčí smlouvě, a/nebo jsou zveřejněné na příslušných webových stránkách dle ustanovení § 219 ZZVZ.
- 13.10 Za důvěrné informace se zejména nepovažují:
- 13.10.1 ujednání této Smlouvy, resp. Dílčí smlouvy, včetně jejích příloh, s výjimkou těch částí, které nejsou uveřejňovány na základě příslušných právních předpisů (obchodní tajemství, osobní údaje, kybernetická bezpečnost a další oblasti),
 - 13.10.2 výše ceny uhrazené za plnění dle této Smlouvy v jednotlivém kalendářním roce.
- 13.11 Bez ohledu na jiná ujednání této Smlouvy je Objednatel oprávněn uveřejnit na příslušných webových stránkách v souladu s ustanovením § 219 ZZVZ:
- 13.11.1 tuto Smlouvu včetně všech jejích změn a dodatků, s výjimkou těch částí, které nejsou uveřejňovány na základě příslušných právních předpisů (obchodní tajemství, osobní údaje, kybernetická bezpečnost),
 - 13.11.2 výši skutečně uhrazené ceny za plnění Veřejné zakázky.
- 13.12 Za porušení povinnosti mlčenlivosti smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v odst.13.3 tohoto článku této Smlouvy, které daná smluvní strana poskytla důvěrné informace druhé smluvní strany.
- 13.13 Ukončení účinnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ujednání tohoto článku této Smlouvy a jejich účinnost včetně ujednání o sankcích přetrvá bez omezení i po ukončení účinnosti této Smlouvy.
- 13.14 Smluvní strany se zavazují, že přijmou taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům a ke zvláštní kategorii osobních údajů, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití.

- 13.15 Poskytovatel se zavazuje dodržovat ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákona č. 110/2019 Sb., o zpracování osobních údajů.

14. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

- 14.1 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy, resp. Dílčí smlouvy.
- 14.2 Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy, resp. Dílčí smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a k prodlení s úhradou jednotlivých peněžních závazků.
- 14.3 Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob dle čl. 12. této Smlouvy a Přílohy č. 3 této Smlouvy, statutárních orgánů smluvních stran, popř. jimi písemně pověřených pracovníků.
- 14.4 Všechna oznámení mezi smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé straně doručena buď osobně, datovou schránkou nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou na titulní stránce této Smlouvy, není-li stanoveno nebo mezi smluvními stranami dohodnuto jinak. Nemá-li komunikace dle předchozí věty mít vliv na platnost a účinnost Smlouvy, připouští se též doručení prostřednictvím e-mailu na čísla a adresy uvedené v Příloze č. 3 této Smlouvy.
- 14.5 Ukládá-li Smlouva doručit některý dokument v písemné podobě, může být doručen buď v tištěné podobě nebo v elektronické (digitální) podobě jako dokument aplikace MS Word verze 2003 nebo vyšší, MS Excel 2003 nebo vyšší či PDF (verze založena na specifikaci ISO 32000-1:2008) na dohodnutém médiu.
- 14.6 Poskytovatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).
- 14.7 Poskytovatel se zavazuje ve lhůtě pěti pracovních dnů ode dne doručení odůvodněné písemné žádosti Objednatele o výměnu oprávněné osoby Poskytovatele podílející se na plnění této Smlouvy, s níž Objednatel nebyl z jakéhokoliv důvodu spokojen, nahradit jinou vhodnou osobou s odpovídající kvalifikací.
- 14.8 Poskytovatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).

15. NÁHRADA ŠKODY

- 15.1 Každá ze stran nese odpovědnost za způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Obě strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

- 15.2 Žádná ze stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé strany. V případě, že Objednatel poskytl Poskytovateli chybné zadání a Poskytovatel s ohledem na svou povinnost poskytovat plnění s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ujednání předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.
- 15.3 Žádná ze smluvních stran není odpovědná za škodu a není ani v prodlení, pokud k tomuto došlo výlučně v důsledku prodlení s plněním závazků druhé smluvní strany nebo v důsledku překážek vylučujících povinnost k náhradě škody ve smyslu ustanovení § 2913 odst. 2 občanského zákoníku (dále jen „**vyšší moc**“).
- 15.4 Za vyšší moc se podle této Smlouvy považují mimořádné nepředvídatelné a nepřekonatelné překážky bránící dočasně nebo trvale plnění povinností stanovených v této Smlouvě, pokud nastaly po jejím uzavření nezávisle na vůli povinné strany a jestliže tyto překážky nemohly být povinnou stranou odvráceny ani při vynaložení veškerého úsilí, které lze rozumně v dané situaci požadovat.
- 15.5 Za vyšší moc se však nepokládají okolnosti, jež vyplývají z osobních nebo hospodářských poměrů povinné strany a dále překážky plnění, které byla příslušná smluvní strana povinna překonat nebo odstranit podle této Smlouvy, obchodních zvyklostí nebo obecně závazných právních předpisů nebo jestliže může důsledky své odpovědnosti smluvně převést na třetí osobu, jakož i okolnosti, které se projeví až v době, kdy povinná strana již byla v prodlení.
- 15.6 Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě škody. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě škody. Každá ze smluvních stran je oprávněna požadovat náhradu škody v plném rozsahu i v případě, že se jedná o porušení povinnosti, na kterou se dle této Smlouvy vztahuje smluvní pokuta nebo sleva z ceny.
- 15.7 Případná náhrada škody bude zaplácena v měně platné na území České republiky, přičemž pro propočítání na tuto měnu je rozhodný kurs České národní banky ke dni vzniku škody.
- 15.8 Každá ze smluvních stran je oprávněna požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta, a to v celém rozsahu.
- 15.9 Škoda se hradí v penězích, případně uvedením do předešlého stavu, podle volby Objednatele v každém konkrétním případě.

16. SANKCE

- 16.1 Poskytovatel je povinen zaplatit Objednateli smluvní pokutu za každý i započatý den prodlení oproti sjednanému termínu řádného a bezvadného poskytnutí Plnění, a to ve výši 5.000,- Kč.
- 16.2 Poskytovatel je povinen zaplatit Objednateli smluvní pokutu za každý i započatý den prodlení oproti sjednanému termínu odstranění závady uvedenému v čl. 6. odst. 6.8 této Smlouvy, a to ve výši 3.000,- Kč.

- 16.3 Poskytovatel je povinen zaplatit Objednateli smluvní pokutu za každý i započatý den prodlení oproti sjednanému termínu odstranění záruční vady uvedenému v čl. 10. odst. 10.7 této Smlouvy, a to ve výši 1.000,- Kč.
- 16.4 Poskytovatel je povinen zaplatit Objednateli smluvní pokutu za porušení povinnosti s přizpůsobením svého ServiceDesku ServiceDesku Objednatele a zajištěním bezproblémové komunikace ServiceDesků navzájem oproti termínu stanoveném v čl. 6. odst. 6.11 této Smlouvy, a to ve výši 3.000,- Kč za každý i započatý den prodlení.
- 16.5 Poruší-li Poskytovatel svůj závazek přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, anebo dojde-li k neoprávněným přenosům osobních údajů nebo k jejich jinému neoprávněnému zpracování ve smyslu ujednání čl. 13. této Smlouvy, jakož i k jinému zneužití osobních údajů, nebo poruší-li Poskytovatel jakýkoliv svůj závazek čl. 13. této Smlouvy, je Objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 200.000,- Kč za každé jednotlivé porušení daného závazku.
- 16.6 Smluvní pokuty mohou být libovolně kombinovány, tzn., uplatnění jedné smluvní pokuty nevylučuje souběžné uplatnění jakékoliv jiné smluvní pokuty.
- 16.7 Uplatněním smluvní pokuty není dotčeno právo Objednatele na náhradu škody způsobené porušením povinnosti Poskytovatelem, na kterou se smluvní pokuta vztahuje.
- 16.8 Smluvní pokuta je splatná do 30 kalendářních dnů ode dne doručení oznámení o uložení smluvní pokuty Poskytovateli.
- 16.9 V případě prodlení s úhradou smluvní pokuty uhradí Poskytovatel Objednateli úrok z prodlení určený nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob a evidence svěřenských fondů a evidence údajů o skutečných majitelích.

17. PLATNOST A ÚČINNOST SMLOUVY

- 17.1 Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem 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) (dále jen „**zákon o registru smluv**“), Objednatelem.
- 17.2 Tato Smlouva se uzavírá na dobu určitou, a to na dobu 4 let ode dne nabytí její účinnosti. Účinnost Dílčí smlouvy může překročit dobu trvání této Smlouvy. V případě předčasného zániku účinnosti této Smlouvy z jakéhokoli důvodu není účinnost Dílčích smluv dotčena, ledaže by se důvod zániku účinnosti Smlouvy vztahoval i na tyto Dílčí smlouvy.
- 17.3 Poskytovatel souhlasí s tím, aby tato Smlouva i Dílčí smlouvy byly uveřejněny v registru smluv v souladu se zákonem o registru smluv.
- 17.4 Smluvní strany souhlasí s tím, aby tato Smlouva byla uveřejněna na profilu zadavatele - Objednatele, jakož i na internetových stránkách Objednatele. Souhlas s uveřejněním podle předchozí věty se nevztahuje na údaje, které jsou obchodním tajemstvím ve smyslu ustanovení § 504 občanského zákoníku, na údaje, jejichž zveřejnění brání

předpisy upravující ochranu osobních údajů, jakož i na údaje, které jsou chráněny před uveřejněním podle jiných právních předpisů.

- 17.5 Smluvní strany prohlašují, že Poskytovatel sdělil Objednateli před podpisem této Smlouvy, zda jsou informace uvedené v této Smlouvě a jejích přílohách obchodním tajemstvím Poskytovatele ve smyslu ustanovení § 504 občanského zákoníku či nikoliv. V případě, že by Poskytovatel trval na tom, že některý údaj obsažený v této Smlouvě a jejích přílohách je obchodním tajemstvím a následně vyšlo najevo, že údaj nenaplníval podmínky stanovené v ustanovení § 504 občanského zákoníku, za nesprávné označení údaje za obchodní tajemství nese odpovědnost Poskytovatel.
- 17.6 Objednatel může od této Smlouvy odstoupit v případě významné změny kontroly nad Poskytovatelem podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, nebo změny nad zásadními aktivy využívanými Poskytovatelem k plnění podle této Smlouvy.
- 17.7 Objednatel může odstoupit od této Smlouvy v souladu s ustanovením § 2001 a násl. Občanského zákoníku. Odstoupení od této Smlouvy je možné mimo jiné v důsledku podstatného porušení této Smlouvy Poskytovatelem. Podstatným porušením této Smlouvy se v tomto případě rozumí zejména porušení povinností ve smyslu ustanovení § 2002 Občanského zákoníku.
- 17.8 Objednatel může odstoupit od této Smlouvy či Dílčí smlouvy zejména v případě, že:
- 17.8.1 Poskytovatel opakovaně (nejméně dvakrát) poskytne vadné plnění, nebo
 - 17.8.2 Poskytovatel je v prodlení s plněním svých povinností déle než 15 kalendářních dní a nezjedná nápravu ani do 10 kalendářních dnů ode dne doručení písemného oznámení Objednatele o takovém prodlení; nebo
 - 17.8.3 dojde k porušení povinnosti ochrany důvěrných informací dle této Smlouvy ze strany Poskytovatele;
 - 17.8.4 na majetek Poskytovatele je prohlášen úpadek, Poskytovatel sám podá dlužnický návrh na zahájení insolvenčního řízení nebo insolvenční návrh je zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení (ve znění insolvenčního zákona); nebo
 - 17.8.5 Poskytovatel vstoupí do likvidace;
 - 17.8.6 Poskytovatel předem neoznámí Objednateli jakoukoliv změnu osoby poddodavatele nebo zvětšení rozsahu plnění svěřeného poddodavateli nebo k takovéto změně Objednatel nedá předem souhlas dle téhož odstavce.
- 17.9 Objednatel je oprávněn od této Smlouvy či Dílčí smlouvy odstoupit rovněž v případě, pokud mu nebudou přiděleny rozpočtové prostředky na financování předmětu plnění dle Smlouvy, resp. příslušné Dílčí smlouvy.
- 17.10 Poskytovatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než 60 kalendářních dnů, pokud Objednatel nezjedná nápravu ani v dodatečně přiměřené lhůtě, kterou mu k tomu Poskytovatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 15 kalendářních dnů od doručení takovéto výzvy.

- 17.11 Účinky odstoupení od této Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
- 17.12 Objednatel je oprávněn tuto Smlouvu nebo Dílčí smlouvu písemně vypovědět (a to i částečně) bez udání důvodů, a to s výpovědní dobou, která uplyne ke konci měsíce následujícího po měsíci doručení písemné výpovědi Poskytovateli. Tuto výpověď nebo částečnou výpověď je Objednatel oprávněn učinit kdykoliv po dobu trvání této Smlouvy.
- 17.13 Ukončením účinnosti této Smlouvy nejsou dotčena ujednání této Smlouvy týkající se licencí, záruk, nároků z odpovědnosti za vady, nároky z odpovědnosti za škodu a ze smluvních pokut, ujednání o ochraně informací, ani další ujednání a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy.
- 17.14 Zánikem účinnosti této Smlouvy není dotčeno vzájemné plnění, pokud bylo řádně poskytnuto, ani práva a nároky z takových plnění vyplývající. V případě, kdy by však Objednatel odstoupil od této Smlouvy z důvodu takového porušení smluvní povinnosti Poskytovatele, že se plnění Poskytovatele stalo pro Objednatele nepotřebným, bude toto plnění Poskytovateli vráceno a ten bude povinen vrátit Objednateli zaplacenou cenu.

18. ŘEŠENÍ SPORŮ

- 18.1 Práva a povinnosti smluvních stran touto Smlouvou výslovně neupravené se řídí občanským zákoníkem a příslušnými právními předpisy souvisejícími.
- 18.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, včetně sporů o její výklad či platnost a usilovat o jejich vyřešení nejprve smírně prostřednictvím jednání oprávněných osob nebo pověřených zástupců. K řešení případných sporů z této Smlouvy je příslušný obecný soud České republiky.

19. ZÁVĚREČNÁ UJEDNÁNÍ

- 19.1 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných osobami oprávněnými jednat jménem smluvních stran, přičemž jakákoliv změna Smlouvy bude provedena v souladu se ZZVZ.
- 19.2 Stane-li se některé z ujednání této Smlouvy neplatné nebo neúčinné, nebude to mít vliv na platnost a účinnost ujednání ostatních a na platnost a účinnost této Smlouvy jakožto celku. Neplatné nebo neúčinné ujednání bude nahrazeno po vzájemné dohodě Smluvních stran takovým ujednáním, které bude odpovídat svým účinkem co nejbližše původnímu záměru a účelu neplatného či neúčinného ujednání v ekonomickém i právním smyslu.
- 19.3 Smluvní strany se dohodly na tom, že právní vztahy vzniklé na základě této Smlouvy se řídí právním řádem České republiky.
- 19.4 Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevyklučuje, na právní nástupce smluvních stran.

19.5 Poskytovatel nesmí postoupit peněžité nároky vůči Objednateli na třetí osobu bez předchozího písemného souhlasu Objednatele.

19.6 Nedílnou součástí této Smlouvy tvoří tyto přílohy:

Příloha č. 1:	Specifikace Zařízení
Příloha č. 2:	Specifikace školení
Příloha č. 3:	Oprávněné osoby
Příloha č. 4:	Seznam poddodavatelů
Příloha č. 5:	Specifikace ceny
Příloha č. 6:	Realizační tým
Příloha č. 7:	Vzor Dílčí smlouvy
Příloha č. 8:	Seznam standardů ČSSZ

19.7 Tato Smlouva je uzavřena elektronicky a je podepsána osobou oprávněnou jednat za Objednatele kvalifikovaným elektronickým podpisem a osobou oprávněnou zastupovat Poskytovatele uznávaným elektronickým podpisem.

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Objednatel

Poskytovatel

V Praze

V Praze

**Ing. Milan
Shrbený**

Digitálně podepsal Ing.
Milan Shrbený
Datum: 2021.02.17
15:05:59 +01'00'

Digitálně podepsal
[redacted]
Datum: 2021.02.02
17:57:18 +01'00'

**Česká republika - Česká správa sociálního
zabezpečení**

ELSO PHILIPS SERVICE spol. s r.o.

Ing. Milan Shrbený

[redacted]
jednatel

ředitel sekce informačních a komunikačních
technologií

Příloha č. 1 Specifikace Zařízení

Prvek_A

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9300-48P-E
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	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Non-stop Forwarding	ANO, povýšením firmware	ANO, povýšením firmware
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Interní redundantní napájecí zdroj požadován instalován v šasi	ANO	ANO
Datový stohovací kabel požadován	ANO	ANO
Napájecí stohovací kabel požadován	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	ANO
Minimální PoE budget	430W	ANO
Uplink porty	4x1GE SFP	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	600	ANO
Min. počet IPv6 routes	300	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	128	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO

Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, povýšením firmware	ANO, povýšením firmware
ISIS	ANO, povýšením firmware	ANO, povýšením firmware
BGPv4	ANO, povýšením firmware	ANO, povýšením firmware
Graceful Insertion and Removal	ANO, povýšením firmware	ANO, povýšením firmware
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	ANO, povýšením firmware
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, povýšením firmware	ANO, povýšením firmware
MPLS VPN	ANO, povýšením firmware	ANO, povýšením firmware
MPLS VPN - 6VPE	ANO, povýšením firmware	ANO, povýšením firmware
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO, povýšením firmware	ANO, povýšením firmware
Reverse path check (uRPF) pro IPv4 i IPv6	ANO, povýšením firmware	ANO, povýšením firmware
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO, povýšením firmware	ANO, povýšením firmware
Minimální počet HW QoS front	8	8
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Per Flow policing	ANO	ANO

QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO, min. 2 úrovně
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	ANO, povýšením firmware
IEEE 802.1ae na uplink portech	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO, povýšením firmware	ANO, povýšením firmware
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	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	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Multicast DNS (mDNS) gateway	ANO, povýšením firmware	ANO, povýšením firmware
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO, povýšením firmware	ANO, povýšením firmware
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ANO, povýšením firmware	ANO, povýšením firmware
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO

SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Application hosting	ANO, povýšením firmware	ANO, povýšením firmware
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO, povýšením firmware	ANO, povýšením firmware
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE) přes IPv4 i IPv6	ANO	ANO
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO, povýšením firmware	ANO, povýšením firmware
NTPv3 server	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení	L2 switch	WS-C2960X-48LPS-L
Formát zařízení	fixní konfigurací, rozšiřitelný na stohování, 1RU	ANO
Stohovatelný bez snížení počtu ethernet portů	ano, volitelným modulem	ANO
Počet portů 10/100/1000	48	ANO
PoE (IEEE 802.3af)	ano	ANO
PoE+ (IEEE 802.3at, 30W/port)	ano	ANO
Dostupný výkon pro napájení PoE portů	min. 350W	ANO
Počet portů 1 Gbit/s a jejich typ	4x SFP	ANO
Možnost připojit externí redundantní zdroj	ano	ANO
Směrovací protokoly	ano	ANO
Výkonnostní parametry		
Minimální propustnost přepínacího subsystému	200 Gbit/s	ANO
Minimální paketový výkon přepínače	100 milionu paketů/vteřinu	ANO
Rychlost stohovacího propojení	alespoň 80 Gbit/s	ANO
Minimální počet MAC adres	15000	ANO
Vlastnosti stohování		
vzájemné stohování všech modelů 10/100 s 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky	ano	ANO
minimální počet přepínačů ve stohu	8	ANO
automatická kontrola a sjednocení verze software přepínačů ve stohu	ano	ANO
možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano	ANO
seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano	ANO
kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano	ANO
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	ANO
IEEE 802.3ad	ano	ANO
Podpora "jumbo rámců"	ano	ANO
Protokoly 2. vrstvy		
IEEE 802.1D	ano	ANO
IEEE 802.1Q	ano	ANO
Minimální počet aktivních VLAN	1000	ANO
Tunelování 802.1Q v 802.1Q	ano	ANO
IEEE 802.1X - Port Based Network Access Control	ano	ANO
IEEE 802.1s - multiple spanning trees	ano	ANO
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	ANO
IEEE 802.1p - Minimální počet vnitřních front	4	ANO
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	ANO
Detekce protilehlého zařízení (např. CDP, LLDP)	ano	ANO
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ano	ANO

Protokol pro definici šířených VLAN (IEEE 802.1ak nebo VTP)	ano	ANO
Detekce jednosměrnosti optické linky (např. UDLD)	ano	ANO
STP root guard	ano	ANO
STP loop guard	ano	ANO
Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)	ano	ANO
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	ANO
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	ANO
QoS	ano	ANO
QoS i na stohovacím propoju	ano	ANO
DHCP relay	ano	ANO
Protokol IPv6		ANO
Certifikace IPv6 ready logo – Phase II	ano	ANO
IPv6 ACL	ano	ANO
IPv6 QoS	ano	ANO
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano	ANO
HTTP, SNMP over IPv6	ano	ANO
RADIUS, TACACS+ over IPv6	ano	ANO
OSPFv3	ano	ANO
IPv6 MLDv2 snooping	ano	ANO
IPv6 Port ACL	ano	ANO
IPv6 First Hop Security RA guard	ano	ANO
IPv6 First Hop Security DHCPv6 guard	ano	ANO
IPv6 First Hop Security IPv6 Binding Integrity Guard	ano	ANO
Směrovací protokoly		ANO
OSPFv2, OSPFv3	ano	ANO
RIPv2	ano	ANO
statické směrování	ano	ANO
Policy-based routing podle ACL	ano	ANO
Směrování multicastu		ANO
PIM	ano	ANO
IGMPv2 snooping	ano	ANO
IGMPv3 snooping	ano	ANO
IPv6 MLDv1 & v2 snooping	ano	ANO
Bezpečnost		ANO
ACL na rozhraní IN/OUT	ano	ANO
ACL pro IP	ano	ANO
ACL pro ethernetové rámce	ano	ANO
IPv6 ACL	ano	ANO
Možnost definovat povolené MAC adresy na portu	ano	ANO
Možnost definovat maximální počet MAC adres na portu	ano	ANO

Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	ANO
DHCP snooping	ano	ANO
Dynamic ARP inspection (DAI)	ano	ANO
Verifikace mapování IP-MAC (např. IP source guard)	ano	ANO
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ano	ANO
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano	ANO
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano	ANO
konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	ANO
ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	ANO
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítě (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ano	ANO
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ano	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloADERu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ano	ANO
Podpora koncových zařízení		ANO
PoE (IEEE 802.3af)	ano	ANO
PoE+ (IEEE 802.3at, 30W/port)	ano	ANO
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano	ANO
Podpora určování polohy klienta, rozšíření WiFi systému pro určování polohy klienta i v pevné LAN síti (například Network Mobility Service Protocol - NMSP)	ano	ANO
EEE (IEEE 802.3az)	ano	ANO
Management		ANO
CLI rozhraní	ano	ANO
SSHv2	ano	ANO
SSHv2 over IPv6	ano	ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ANO
SNMPv2	ano	ANO
SNMPv3	ano	ANO
USB konzolová linka	ano	ANO
Sériová konzolová linka	ano	ANO
10/100 management out-of-band port	ano	ANO
DNS klient	ano	ANO
NTP klient s MD5 autentizací	ano	ANO
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	ANO
Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače	ano	ANO

Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ano	ANO
Statistiky určovány z každého paketu daného "flow"	ano, povýšením firmware	ano, povýšením firmware
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano	ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	ANO
TACACS+ klient	ano	ANO
Port mirroring (SPAN)	ano	ANO
port mirroring 1 -> 1	ano	ANO
port mirroring N -> 1	ano	ANO
port mirroring ACL (mirroruje pouze definované toky)	ano	ANO
Vzdálený port mirroring (RSPAN)	ano	ANO
Syslog	ano	ANO
Měření zakončení a délky metalického kabelu (TDR)	ano	ANO
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ano	ANO
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano	ANO
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ano	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano	ANO
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano	ANO
Služby		
DHCP server	ano	ANO

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_B1	Stohovací modul metalický	min. 2 porty (metalické)	C2960X-STACK=	ANO
Modul_B2	Stohovací modul kombinovaný (metalický + optický)	min. 2 porty (metalický + optický SFP+)	C2960X-HYBRID-STK=	ANO
Modul_B3	Stohovací modul optický	min. 2 porty (optické SFP+)	C2960X-FIBER-STK=	ANO
Modul_B4	Stohovací datový kabel metalický	min. 0,5m	CAB-STK-E-0.5M=	ANO
Modul_B5	Stohovací datový kabel metalický	min. 1m	CAB-STK-E-1M=	ANO
Modul_B6	Stohovací datový kabel metalický	min. 3m	CAB-STK-E-3M=	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení	L3 switch	WS-C3650-48PS-S
Formát zařízení	fixní konfigurací, stohovatelný, 1RU	ano
Stohovatelný bez snížení počtu ethernet portů	ano	ano
Počet portů 10/100/1000	48	ano
PoE (IEEE 802.3af)	ano	ano
PoE+ (IEEE 802.3at, 30W/port)	ano	ano
Dostupný výkon pro napájení PoE portů	min. 370W	ano
Počet portů 1 Gbit/s a jejich typ	4xSFP	ano
Možnost osadit redundantní interní napájecí zdroj, vyměnitelný za chodu	ano	ano
Možnost kombinace AC a DC zdroje v jednom zařízení	ano	ano
Redundantní ventilátor	ano	ano
Směrovací protokoly	ano	ano
Výkonnostní parametry		
Minimální propustnost přepínacího subsystému	170 Gbit/s	ano
Minimální paketový výkon přepínače	70 milionu paketů/vteřinu	ano
Rychlost stohovacího propojení	alespoň 150 Gbit/s	ano
Minimální počet MAC adres	30000	ano
Vlastnosti stohování		
vzájemné stohování všech modelů 10/100 s 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky	ano	ano
minimální počet přepínačů ve stohu	9	ano
automatická kontrola a sjednocení verze software přepínačů ve stohu	ano	ano
možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano	ano
seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano	ano
kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano	ano
synchronizace všech stavů mezi aktivním řídicím prvkem a jedním ze záložních pro minimalizaci vlivu výpadků	ano	ano
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	ano
IEEE 802.3ad	ano	ano
Podpora "jumbo rámců"	ano	ano
Protokoly 2. vrstvy		
IEEE 802.1D	ano	ano
IEEE 802.1Q	ano	ano
Minimální počet aktivních VLAN	4000	ano
Tunelování 802.1Q v 802.1Q	ano	ano
IEEE 802.1X - Port Based Network Access Control	ano	ano

IEEE 802.1s - multiple spanning trees	ano	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	ano
IEEE 802.1p - Minimální počet vnitřních front	8	ano
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	ano
Detekce protilehlého zařízení (např. CDP, LLDP)	ano	ano
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ano	ano
Protokol pro definici šířených VLAN (IEEE 802.1ak nebo VTP)	ano	ano
Detekce jednosměrnosti optické linky (např. UDLD)	ano	ano
STP root guard	ano	ano
STP loop guard	ano	ano
Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)	ano	ano
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	ano
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	ano
QoS	ano	ano
QoS i na stohovacím propoji	ano	ano
možnost konfigurovat QoS na stohovacím propoji	ano	ano
DHCP relay	ano	ano
Protokol IPv6		ano
Certifikace IPv6 ready logo – Phase II	ano	ano
HSRP nebo VRRP pro IPv6	ano	ano
IPv6 ACL	ano	ano
IPv6 QoS	ano	ano
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano	ano
HTTP, SNMP over IPv6	ano	ano
RADIUS, TACACS+ over IPv6	ano	ano
OSPFv3	ano	ano
IPv6 MLDv2 snooping	ano	ano
IPv6 Port ACL	ano	ano
IPv6 First Hop Security RA guard	ano	ano
IPv6 First Hop Security DHCPv6 guard	ano	ano
IPv6 First Hop Security IPv6 SourceGuard	ano	ano
IPv6 First Hop Security IPv6 Binding Integrity Guard	ano	ano
DHCPv6 Server and Relay	ano	ano
Směrovací protokoly		
BGPv4	ano, povýšením software	ano, povýšením software
OSPFv2, OSPFv3	ano	ano
OSPF s MD5 a NSSA	ano	ano
RIPv2	ano	ano

statické směrování	ano	ano
Policy-based routing podle ACL	ano	ano
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ano, povýšením software	ano, povýšením software
Virtualizace směrovacích funkcí (např. Multi-VRF)	ano	ano
Směrování multicastu		
PIM (dense i sparse mód)	ano, povýšením software	ano, povýšením software
IGMPv2 snooping	ano	ano
IGMPv3 snooping	ano	ano
IPv6 MLDv1 & v2 snooping	ano	ano
Bezpečnost		
Reverse path check (uRPF)	ano	ano
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.3ad)	ano	ano
ACL pro IP	ano	ano
ACL pro ethernetové rámce	ano	ano
IPv6 ACL	ano	ano
Možnost definovat povolené MAC adresy na portu	ano	ano
Možnost definovat maximální počet MAC adres na portu	ano	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	ano
DHCP snooping	ano	ano
Dynamic ARP inspection (DAI)	ano	ano
Verifikace mapování IP-MAC (např. IP source guard)	ano	ano
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ano	ano
Šifrování na L2 dle IEEE 802.1AE	ano	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano	ano
konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	ano
ověřování dle IEEE 802.1x volitelně bez omezení přístupu (pro monitoring a snadné nasazení 802.1x)	ano	ano
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ano	ano
Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)	ano	ano
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ano	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	ano
Podpora SUDI (IEEE 802.1AR) autentizace	ano	ano
Podpora koncových zařízení		
PoE (IEEE 802.3af)	ano	ano
PoE+ (IEEE 802.3at, 30W/port)	ano	ano
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano	ano
Podpora určování polohy klienta, rozšíření WiFi systému pro určování polohy klienta i v pevné LAN síti (například Network Mobility Service Protocol - NMSP)	ano	ano
EEE (IEEE 802.3az)	ano	ano
Inzerce služeb pomocí Apple Bonjour protokolu i mezi VLANy	ano	ano
Management		
CLI rozhraní	ano	ano
SSHv2	ano	ano
SSHv2 over IPv6	ano	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ano
SNMPv2	ano	ano
SNMPv3	ano	ano
Netconf a YANG	ano	ano
USB konzolová linka	ano	ano
Sériová konzolová linka	ano	ano
10/100 management out-of-band port	ano	ano
DNS klient	ano	ano
NTP klient s MD5 autentizací	ano	ano
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	ano
Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače	ano	ano
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ano	ano
Statistiky určovány z každého paketu daného "flow"	ano	ano
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano	ano
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"	ano	ano
Zobrazení sbíraných informací o "flow" přímo v přepínači. I včetně "TopN" pohledu.	ano	ano
Export statistik "flow" selektivně na více kolektorů	ano	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	ano
TACACS+ klient	ano	ano
Port mirroring (SPAN)	ano	ano
port mirroring 1 -> 1	ano	ano
port mirroring N -> 1	ano	ano
port mirroring ACL (mirroruje pouze definované toky)	ano	ano

Vzdálený port mirroring (RSPAN)	ano	ano
Vzdálený port mirroring přes L3 síť/WAN (např. ERSPAN nebo ekvivalentní)	ano	ano
Syslog	ano	ano
Měření zakončení a délky metalického kabelu (TDR)	ano	ano
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ano	ano
Interpret jazyka Python přímo v zařízení	ano	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano	ano
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano	ano
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ano	ano
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ano	ano
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano	ano
Služby		
NTP server	ano	ano
DHCP server	ano	ano

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_C1	Napájecí AC zdroj	min. 600W	PWR-C2-640WAC=	ANO
Modul_C2	Napájecí AC zdroj	min. 1000W	PWR-C2-1025WAC=	ANO
Modul_C3	Stohovací modul metalický	min. 2 porty (metalické)	C3650-STACK-KIT=	ANO
Modul_C4	Stohovací datový kabel	min. 0,5m	STACK-T2-50CM=	ANO
Modul_C5	Stohovací datový kabel	min. 1m	STACK-T2-1M=	ANO
Modul_C6	Stohovací datový kabel	min. 3m	STACK-T2-3M=	ANO
Modul_C7	Povýšení firmware o specifikované povýšitelné funkce	ANO	L-C3650-48-S-E	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení	L3 switch	WS-C3850-12XS-S
Formát zařízení	fixní konfigurací, 1RU	ano
Stohovatelný bez snížení počtu ethernet portů	ano	ano
Stohování požadováno	ano	ano
Počet portů 10 Gbit/s a jejich typ	12x SFP+	ano
možnost volby 1Gbit/s nebo 10Gbit/s rychlosti uplink portu vhodným rozšiřujícím modulem a transcieverem	ano	ano
Možnost rozšíření o redundantní interní napájecí zdroj, vyměnitelný za chodu	ano	ano
Možnost kombinace AC a DC zdroje v jednom zařízení	ano	ano
Možnost připojit externí redundantní zdroj	ano	ano
Redundantní ventilátor	ano	ano
Směrovací protokoly	ano	ano
Integrovaná funkcionalita WiFi kontroleru	ano	ano
Podpora distribuovaných bezdrátových vlastností (mobility) v přepínači, řízených centrálním kontrolerem	ano	ano
Výkonnostní parametry		
Minimální propustnost přepínacího subsystému	300 Gbit/s	ano
Minimální paketový výkon přepínače	220 milionu paketů/vteřinu	ano
Rychlost stohovacího propojení	alespoň 460 Gbit/s	ano
Minimální počet MAC adres	30000	ano
Vlastnosti stohování		
sdílení výkonu napájecích zdrojů napříč celým stohem	ano	ano
vzájemné stohování všech modelů 10/100 s 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky	ano	ano
minimální počet přepínačů ve stohu	9	ano
automatická kontrola a sjednocení verze software přepínačů ve stohu	ano	ano
možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano	ano
seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano	ano
kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano	ano
synchronizace všech stavů mezi aktivním řídicím prvkem a jedním ze záložních pro minimalizaci vlivu výpadků	ano	ano
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	ano
IEEE 802.3ad	ano	ano
Podpora "jumbo rámců"	ano	ano
Protokoly 2. vrstvy		
IEEE 802.1D	ano	ano
IEEE 802.1Q	ano	ano
Minimální počet aktivních VLAN	1000	ano
Tunelování 802.1Q v 802.1Q	ano	ano
IEEE 802.1X - Port Based Network Access Control	ano	ano
IEEE 802.1s - multiple spanning trees	ano	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	ano
IEEE 802.1p - Minimální počet vnitřních front	8	ano
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	ano

Detekce protilehlého zařízení (např. CDP, LLDP)	ano	ano
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ano	ano
Protokol pro definici šířených VLAN (IEEE 802.1ak nebo VTP)	ano	ano
Detekce jednosměrnosti optické linky (např. UDLD)	ano	ano
STP root guard	ano	ano
STP loop guard	ano	ano
Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)	ano	ano
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	ano
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	ano
QoS	ano	ano
QoS i na stohovacím propoji	ano	ano
možnost konfigurovat QoS na stohovacím propoji	ano	ano
DHCP relay	ano	ano
Protokol IPv6		
Certifikace IPv6 ready logo – Phase II	ano	ano
HSRP nebo VRRP pro IPv6	ano	ano
IPv6 ACL	ano	ano
IPv6 QoS	ano	ano
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano	ano
HTTP, SNMP over IPv6	ano	ano
RADIUS, TACACS+ over IPv6	ano	ano
OSPFv3	ano	ano
IPv6 MLDv2 snooping	ano	ano
IPv6 Port ACL	ano	ano
IPv6 First Hop Security RA guard	ano	ano
IPv6 First Hop Security DHCPv6 guard	ano	ano
IPv6 First Hop Security IPv6 SourceGuard	ano	ano
IPv6 First Hop Security IPv6 Binding Integrity Guard	ano	ano
DHCPv6 Server and Relay	ano	ano
Směrovací protokoly		
BGPv4	ano, povýšením software	ano
OSPFv2, OSPFv3	ano	ano
OSPF s MD5 a NSSA	ano	ano
RIPv2	ano	ano
statické směrování	ano	ano
Policy-based routing podle ACL	ano	ano
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ano, povýšením software	ano
Virtualizace směrovacích funkcí (např. Multi-VRF)	ano	ano
Směrování multicastu		
PIM (dense i sparse mód)	ano, povýšením software	ano
PIM		ano
IGMPv2 snooping	ano	ano
IGMPv3 snooping	ano	ano
IPv6 MLDv1 & v2 snooping	ano	ano

Bezpečnost		
Reverse path check (uRPF)	ano	ano
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.3ad)	ano	ano
ACL pro IP	ano	ano
ACL pro ethernetové rámce	ano	ano
IPv6 ACL	ano	ano
Možnost definovat povolené MAC adresy na portu	ano	ano
Možnost definovat maximální počet MAC adres na portu	ano	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	ano
DHCP snooping	ano	ano
Dynamic ARP inspection (DAI)	ano	ano
Verifikace mapování IP-MAC (např. IP source guard)	ano	ano
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ano	ano
Šifrování na L2 dle IEEE 802.1AE	ano	ano
Šifrování na L2 dle IEEE 802.1AE, AES s délkou klíče 256 bitů	ano	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano	ano
konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	ano
ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	ano
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag	ano	ano
Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám	ano	ano
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ano	ano
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje	ano	ano
Podpora SUDI (IEEE 802.1AR) autentizace	ano	ano
Podpora koncových zařízení		
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano	ano
Podpora určování polohy klienta, rozšíření WiFi systému pro určování polohy klienta i v pevné LAN síti (například Network	ano	ano
EEE (IEEE 802.3az)	ano	ano
Inzerce služeb pomocí Apple Bonjour protokolu i mezi VLANy	ano	ano
Management		
CLI rozhraní	ano	ano
SSHv2	ano	ano
SSHv2 over IPv6	ano	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ano
SNMPv2	ano	ano
SNMPv3	ano	ano
Netconf a YANG	ano	ano
USB konzolová linka	ano	ano
Sériová konzolová linka	ano	ano
10/100 management out-of-band port	ano	ano
DNS klient	ano	ano
NTP klient s MD5 autentizací	ano	ano
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	ano
Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače	ano	ano
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ano	ano

Statistiky určované z každého paketu daného "flow"	ano	ano
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano	ano
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"	ano	ano
Zobrazení sbíraných informací o "flow" přímo v přepínači. I včetně "TopN" pohledu.	ano	ano
Export statistik "flow" selektivně na více kolektorů	ano	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	ano
TACACS+ klient	ano	ano
Port mirroring (SPAN)	ano	ano
port mirroring 1 -> 1	ano	ano
port mirroring N -> 1	ano	ano
port mirroring ACL (mirroruje pouze definované toky)	ano	ano
Vzdálený port mirroring (RSPAN)	ano	ano
Vzdálený port mirroring přes L3 síť/WAN (např. ERSPAN nebo ekvivalentní)	ano	ano
Syslog	ano	ano
Měření zakončení a délky metalického kabelu (TDR)	ano	ano
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ano	ano
Interpret jazyka Python přímo v zařízení	ano	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano	ano
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano	ano
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ano	ano
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ano	ano
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano	ano
Služby		
NTP server	ano	ano
DHCP server	ano	ano

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_D1	Optický rozšiřující modul 10GE	min. 4x 10GE	C3850-NM-4-10G=	ANO
Modul_D2	Napájecí AC zdroj	min. 330W	PWR-C1-350WAC=	ANO
Modul_D3	Povýšení firmware o specifikované povýšitelné funkce	ANO	L-C3850-12-S-E	ANO

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9200L-24P-4G-E
Formát přepínače	Stohovatelný	ANO
Stohování požadováno	ANO	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	80 Gb/s	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Redundantní ventilátory	ANO	ANO
Interní redundantní napájecí zdroj požadován	NE	ANO
Datový stohovací kabel požadován	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE+ napájením	24	ANO
Minimální PoE budget	350W	ANO
Uplink porty	4x1GE SFP	ANO
Min. velikost sdíleného systémového bufferu	6MB	ANO
Velikost MAC address tabulky	16000	ANO
Min. počet IPv4 routes	600	ANO
Min. počet IPv6 routes	300	ANO
Min. počet konfigurovatelných security ACL	1000	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO

RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, povýšením firmware	ANO, povýšením firmware
ISIS	ANO, povýšením firmware	ANO, povýšením firmware
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	ANO, povýšením firmware
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (SSH, Syslog)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VAACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	ANO, povýšením firmware
IEEE 802.1ae na uplink portech	ANO	ANO

Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE)	ANO	ANO

Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_E1	Stohovací datový kabel	min. 1m	STACK-T4-1M	ANO
Modul_E2	Stohovací datový kabel	min. 3m	STACK-T4-3M	ANO
Modul_E3	Povýšení firmware o specifikované povýšitelné funkce	ANO	C9200L-24-E-A-3	ANO

Požadovaná funkcionální/vlastnost	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9407R-96U-BNDL-E
Formát přepínače	modulární	ANO
Počet slotů v šasi pro moduly rozhraní	5	ANO
Výška šasi	max. 10RU	ANO
Hloubka šasi	max. 43cm	ANO
Požadovaný počet portů 10/100/1000 s 60W PoE	96	ANO
Redundantní zdroje v režimu N+1 i N+N	ANO	ANO
Požadovaný režim redundantních zdrojů	N+1	ANO
Požadovaný počet napájecích zdrojů	2	ANO
Napájecí zdroje, max.dosažitelný výkon každého	min. 3000W	ANO
ventilátory vyměnitelné z přední strany šasi	ANO	ANO
ventilátory vyměnitelné ze zadní strany šasi	ANO	ANO
Počet a typ uplink slotů z řídicího modulu	8x10GE+2x40GE	ANO
Požadovaná minimální přenosová kapacita slotu	80 Gbit/s	ANO
Možnost redundantního řídicího modulu	ANO	ANO
Výpadek redundantního řídicího modulu nesmí snížit přenosovou kapacitu přepínače	ANO	ANO
Stateful Switch Over	ANO	ANO
Non-stop Forwarding mezi řídicími moduly	ANO, zvýšením firmware	ANO, zvýšením firmware
ISSU	ANO, zvýšením firmware	ANO, zvýšením firmware
Min. velikost sdíleného systémového bufferu	96MB	ANO
Velikost MAC address tabulky	60000	ANO
Min. počet IPv4 routes	600	ANO
Min. počet IPv6 routes	300	ANO
Min. počet konfigurovatelných security ACL záznamů	16000	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více karet v šasi	ANO	ANO
IEEE 802.3ad přes více šasi	ANO, zvýšením firmware	ANO, zvýšením firmware
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	64	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet VLAN ID	4000	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, zvýšením firmware	ANO, zvýšením firmware
ISIS	ANO, zvýšením firmware	ANO, zvýšením firmware
BGPv4	ANO, zvýšením firmware	ANO, zvýšením firmware
Graceful Insertion and Removal	ANO, zvýšením firmware	ANO, zvýšením firmware
IP Multicast (PIM SSM, PIM SM)	ANO, zvýšením firmware	ANO, zvýšením firmware
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, zvýšením firmware	ANO, zvýšením firmware
MPLS VPN	ANO, zvýšením firmware	ANO, zvýšením firmware

MPLS VPN - 6VPE	ANO, povýšením firmware	ANO, povýšením firmware
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Per Flow policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VAACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	ANO, povýšením firmware
IEEE 802.1AE na všech portech	ANO	ANO
IEEE 802.1ae (AES-GCM-256)	ANO, povýšením firmware	ANO, povýšením firmware
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která overuje autentičnost a integritu jak bootloADERu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Multicast DNS (mDNS) gateway	ANO, povýšením firmware	ANO, povýšením firmware
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO, povýšením firmware	ANO, povýšením firmware

Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ANO, povýšením firmware	ANO, povýšením firmware
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace komponent zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní události v systému zařízení	ANO	ANO
Application hosting	ANO	ANO
Aplikace softwarových záplat, nikoli povýšování celého firmware	ANO, povýšením firmware	ANO, povýšením firmware
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE) přes IPv4 i IPv6	ANO	ANO
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO, povýšením firmware	ANO, povýšením firmware
NTPv3 server	ANO	ANO

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_F1	Povýšení firmware o specifikované povýšitelné funkce	ANO	C9400-DNA-E-A-3	ANO
Modul_F2	Redundantní řídicí modul 8x10GE a 2x40GE sloty	min. 80 Gbit/s kapacita na slot	C9400-SUP-1=	ANO
Modul_F3	Metalický rozšiřující modul 10/100/1000 ethernet	min. 48x 10/100/1000	C9400-LC-48T=	ANO
Modul_F4	Metalický rozšiřující modul 10/100/1000 ethernet, IEEE 802.3at na všech portech	min. 48x 10/100/1000	C9400-LC-48P=	ANO
Modul_F5	Metalický rozšiřující modul 10/100/1000 ethernet, s podporou 2,5G/5G/10Gbase-T ethernet, PoE 60W na port, 802.3at (PoE+) na všech portech současně	min. 24x 10/100/1000 a min. 24x 100/1G/2,5G/5G/10Gbase-T	C9400-LC-48UX=	ANO
Modul_F6	Optický rozšiřující modul s 1GE (SFP) sloty	min. 24x 1GE SFP+	C9400-LC-24S=	ANO
Modul_F7	Optický rozšiřující modul s 1GE (SFP) sloty	min. 48x 1GE SFP+	C9400-LC-48S=	ANO
Modul_F8	Optický rozšiřující modul s 1GE/10GE (SFP/SFP+) sloty	min. 24x 10GE SFP+	C9400-LC-24XS=	ANO
Modul_F9	Napájecí zdroj, 220V	min. 3000 W	C9400-PWR-3200AC=	ANO
Modul_F10	Napájecí zdroj, 220V	min. 2000 W	C9400-PWR-2100AC=	ANO

Požadovaná funkcionální/vlastnost	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9500-24Y4C-A
Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28	24	ANO
Možnost volby rychlosti 40/100GE na rozhraních typu QSFP28	ANO	ANO
Uplink porty	4x100GE QSFP28	ANO
Interní redundantní napájecí zdroj instalovaný v zařízení	ANO	ANO
Min. velikost sdíleného systémového bufferu	36MB	ANO
Velikost MAC address tabulky	80000	ANO
Min. počet IPv4 routes	100000	ANO
Min. počet IPv6 routes	100000	ANO
Min. počet konfigurovatelných security ACL	27000	ANO
Flexibilní alokace SRAM a TCAM zdrojů	ANO	ANO
IEEE 802.3ad (Link Aggregation - LAG)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimální počet aktivních VLAN	4000	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
Podpora jumbo rámců (min. 9216 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO	ANO
ISIS	ANO	ANO
BGPv4	ANO	ANO
Graceful Insertion and Removal	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	10	ANO
MPLS VPN	ANO	ANO
MPLS VPN - 6VPE	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
Reverse path check (uRPF)	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS - Strict Priority Queue	ANO	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO

QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
Port ACL, VLAN ACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloADERu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovaných klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.1AE na všech portech	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na všech portech	ANO	ANO
Source-Group Tag Exchange Protocol nebo ekvivalentní	ANO	ANO
IGMPv2/v3 snooping	ANO	ANO
MLD snooping	ANO	ANO
Multicast DNS (mDNS) gateway	ANO	ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Application hosting	ANO	ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO	ANO
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

Požadovaná funkcionálnita/vlastnost	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9407R
Formát přepínače	modulární	ANO
Počet slotů v šasi pro moduly rozhraní	5	ANO
Výška šasi	max. 10RU	ANO
Hloubka šasi	max. 43cm	ANO
Redundantní zdroje v režimu N+1 i N+N	ANO	ANO
Požadovaný režim redundantních zdrojů	N+1	ANO
Požadovaný počet napájecích zdrojů	2	ANO
Napájecí zdroje, max.dosažitelný výkon každého	min. 3000W	ANO
ventilátory vyměnitelné z přední strany šasi	ANO	ANO
ventilátory vyměnitelné ze zadní strany šasi	ANO	ANO
Počet a typ uplink slotů z řídicího modulu	8x10GE+2x40GE	ANO
Požadovaná minimální přenosová kapacita slotu	120 Gbit/s	ANO
Možnost redundantního řídicího modulu	ANO	ANO
Výpadek redundantního řídicího modulu nesmí snížit přenosovou kapacitu přepínače	ANO	ANO
Stateful Switch Over	ANO	ANO
Non-stop Forwarding mezi řídicími moduly	ANO	ANO
ISSU	ANO	ANO
Min. velikost sdíleného systémového bufferu	96MB	ANO
Velikost MAC address tabulky	60000	ANO
Min. počet IPv4 routes	100000	ANO
Min. počet IPv6 routes	50000	ANO
Min. počet konfigurovatelných security ACL záznamů	16000	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více karet v šasi	ANO	ANO
IEEE 802.3ad přes více šasi	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	64	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet VLAN ID	4000	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO

EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO	ANO
ISIS	ANO	ANO
BGPv4	ANO	ANO
Graceful Insertion and Removal	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
MPLS VPN	ANO	ANO
MPLS VPN - 6VPE	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Per Flow policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VAACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO	ANO
IEEE 802.1AE na všech portech	ANO	ANO
IEEE 802.1ae (AES-GCM-256)	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO

Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloADERu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Multicast DNS (mDNS) gateway	ANO	ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášovaných aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace komponent zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Application hosting	ANO	ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO	ANO
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE) přes IPv4 i IPv6	ANO	ANO
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_H1	Redundantní řídicí modul 8x10GE a 2x40GE sloty	min. 120 Gbit/s kapacita na slot	C9400-SUP-1XL=	ANO
Modul_H2	Optický rozšiřující modul s 1GE/10GE (SFP/SFP+) sloty	min. 24x 10GE SFP+	C9400-LC-24XS=	ANO
Modul_H3	Optický rozšiřující modul s 1GE (SFP) sloty	min. 48x 1GE SFP	C9400-LC-48S=	ANO
Modul_H4	Optický rozšiřující modul s 1GE (SFP) sloty	min. 24x 1GE SFP	C9400-LC-24S=	ANO
Modul_H5	Metalický rozšiřující modul 10/100/1000 ethernet, s podporou 2,5G/5G/10Gbase-T ethernet, PoE 60W na port, 802.3at (PoE+) na všech portech současně	min. 24x 10/100/1000 a min. 24x 100/1G/2,5G/5G/10Gbase-T	C9400-LC-48UX=	ANO
Modul_H6	Metalický rozšiřující modul 10/100/1000 ethernet	min. 48x 10/100/1000	C9400-LC-48T=	ANO

Požadovaná funkcionální/vlastnost	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9200L-48T-4G-E
Formát přepínače	Stohovatelný	ANO
Stohování požadováno	ANO	ANO
Stohování s minimálním počtem dedikovaných stohovacích portů	2	ANO
Stohování s minimálním počtem zařízení ve stohu	8	ANO
Stohování s minimální kapacitou sběrnice stohu	80 Gb/s	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Redundantní ventilátory	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE+ napájením	48	ANO
Minimální PoE budget	700W	ANO
Uplink porty	4x1GE SFP	ANO
Min. velikost sdíleného systémového bufferu	6MB	ANO
Velikost MAC address tabulky	16000	ANO
Min. počet IPv4 routes	600	ANO
Min. počet IPv6 routes	300	ANO
Min. počet konfigurovatelných security ACL	1000	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, povýšením firmware	ANO, povýšením firmware
ISIS	ANO, povýšením firmware	ANO, povýšením firmware
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	ANO, povýšením firmware

First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (SSH, Syslog)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VAACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	ANO, povýšením firmware
IEEE 802.1ae na uplink portech	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloADERu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO

CLI rozhraní	ANO	ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE)	ANO	ANO
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_I1	Stohovací datový kabel	min. 1m	STACK-T4-1M=	ANO
Modul_I2	Stohovací datový kabel	min. 3m	STACK-T4-3M=	ANO
Modul_I3	Povýšení firmware o specifikované povýšitelné funkce	ANO	C9200L-48-E-A-3	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení	L3 switch	WS-C3560CX-12PD-S
Formát zařízení	fixní konfigurací, 1RU, kompaktní rozměry, bezventilátorový	ano
Počet portů 10/100/1000	12	ano
PoE (IEEE 802.3af)	Ano, na všech 10/100/1000 portech	ano
PoE+ (IEEE 802.3at, 30W/port)	Ano, na všech 10/100/1000 portech	ano
Dostupný výkon pro napájení PoE portů	min. 200W	ano
Počet portů 1 Gbit/s a jejich typ	2x 1000 Base-T	ano
Počet portů 10 Gbit/s a jejich typ	2x SFP+	ano
možnost volby 1Gbit/s nebo 10Gbit/s rychlosti uplink portu vhodným rozšiřujícím modulem a transcieverem	ano	ano
Bezventilátorový provoz	ano	ano
Směrovací protokoly	ano	ano
Výkonnostní parametry		
Minimální propustnost přepínacího subsystému	68 Gbit/s	ano
Minimální paketový výkon přepínače	50 milionu paketů/vteřinu	ano
Rychlost stohovacího propojení	alespoň 20 Gbit/s	ano
Minimální počet MAC adres	15000	ano
Vlastnosti stohování		
minimální počet přepínačů ve stohu	8	ano
seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano	ano
kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano	ano
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	ano
IEEE 802.3ad	ano	ano
Podpora "jumbo rámců"	ano	ano
Protokoly 2. vrstvy		
IEEE 802.1D	ano	ano
IEEE 802.1Q	ano	ano
Minimální počet aktivních VLAN	1000	ano
Tunelování 802.1Q v 802.1Q	ano	ano
IEEE 802.1X - Port Based Network Access Control	ano	ano
IEEE 802.1s - multiple spanning trees	ano	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	ano
IEEE 802.1p - Minimální počet vnitřních front	ano	ano
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	ano
Detekce protilehlého zařízení (např. CDP, LLDP)	ano	ano
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ano	ano
Protokol pro definici šířených VLAN (IEEE 802.1ak nebo VTP)	ano	ano
Detekce jednosměrnosti optické linky (např. UDLD)	ano	ano
STP root guard	ano	ano
STP loop guard	ano	ano

Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)	ano	ano
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	ano
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	ano
QoS	ano	ano
DHCP relay	ano	ano
Protokol IPv6		
Certifikace IPv6 ready logo – Phase II	ano	ano
HSRP nebo VRRP pro IPv6	ano	ano
IPv6 ACL	ano	ano
IPv6 QoS	ano	ano
IPv6 services (Telnet, SSH, Syslog, ICMP)	ano	ano
HTTP, SNMP over IPv6	ano	ano
RADIUS, TACACS+ over IPv6	ano	ano
OSPFv3	ano	ano
IPv6 MLDv2 snooping	ano	ano
IPv6 Port ACL	ano	ano
IPv6 First Hop Security RA guard	ano	ano
IPv6 First Hop Security DHCPv6 guard	ano	ano
IPv6 First Hop Security IPv6 SourceGuard	ano	ano
IPv6 First Hop Security IPv6 Binding Integrity Guard	ano	ano
DHCPv6 Server and Relay	ano	ano
Směrovací protokoly		
BGPv4	ano, povýšením firmware	ano, povýšením firmware
OSPFv2, OSPFv3	ano	ano
OSPF s MD5 a NSSA	ano, povýšením firmware	ano, povýšením firmware
RIPv2	ano	ano
statické směrování	ano	ano
Policy-based routing podle ACL	ano	ano
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ano, povýšením firmware	ano, povýšením firmware
Směrování multicastu		
PIM (dense i sparse mód)	ano, povýšením firmware	ano, povýšením firmware
IGMPv2 snooping	ano	ano
IGMPv3 snooping	ano	ano
IPv6 MLDv1 & v2 snooping	ano	ano
Bezpečnost		
Reverse path check (uRPF)	ano	ano
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.3ad)	ano	ano
ACL pro IP	ano	ano
ACL pro ethernetové rámce	ano	ano
IPv6 ACL	ano	ano
Možnost definovat povolené MAC adresy na portu	ano	ano
Možnost definovat maximální počet MAC adres na portu	ano	ano

Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	ano
DHCP snooping	ano	ano
Dynamic ARP inspection (DAI)	ano	ano
Verifikace mapování IP-MAC (např. IP source guard)	ano	ano
Ochrana centrálního procesoru (control plane) před útoky typu DoS		
Šifrování na L2 dle IEEE 802.1AE	ano	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano	ano
konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	ano
ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	ano
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ano	ano
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního svstému zařízení prostřednictvím interních HW prostředků	ano	ano
Podpora koncových zařízení		
PoE (IEEE 802.3af)	ano	ano
PoE+ (IEEE 802.3at, 30W/port)	ano	ano
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano	ano
EEE (IEEE 802.3az)	ano	ano
Management		
CLI rozhraní	ano	ano
SSHv2	ano	ano
SSHv2 over IPv6	ano	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ano
SNMPv2	ano	ano
SNMPv3	ano	ano
USB konzolová linka	ano	ano
Sériová konzolová linka	ano	ano
DNS klient	ano	ano
NTP klient s MD5 autentizací	ano	ano
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	ano
Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače	ano	ano
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ano	ano
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	ano
TACACS+ klient	ano	ano
Port mirroring (SPAN)	ano	ano
port mirroring 1 -> 1	ano	ano
port mirroring ACL (mirroruje pouze definované toky)	ano	ano

Vzdálený port mirroring (RSPAN)	ano	ano
Syslog	ano	ano
Měření zakončení a délky metalického kabelu (TDR)	ano	ano
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ano	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano	ano
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano	ano
Nástroje pro pasivní monitorování i aktivní testování odezev provozovaných aplikací (např. IP SLA Video Operation, performance monitor nebo ekvivalentní)	ano	ano
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ano	ano
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano	ano
Služby		
DHCP server	ano	ano

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_J1	Uchycení prvku do 19' racku	ANO	RCKMNT-19-CMPCT	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ přepínače	L2/L3 přepínač	C9200-48P-E
Formát přepínače	Stohovatelný	ANO
Stohování požadováno	ANO	ANO
Stohování s minimálním počtem dedikovaných stohovacích portů	2	ANO
Stohování s minimálním počtem zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	160 Gb/s	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Interní redundantní napájecí zdroj instalovaný v zařízení	ANO	ANO
Možnost povyšovat uplink modul	ANO	ANO
Redundantní ventilátory	ANO	ANO
Redundantní ventilátory vyměnitelné za chodu zařízení	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE+ napájením	48	ANO
Minimální PoE budget	700W	ANO
Min. velikost sdíleného systémového bufferu	6MB	ANO
Velikost MAC address tabulky	32000	ANO
Min. počet IPv4 routes	600	ANO
Min. počet IPv6 routes	300	ANO
Min. počet konfigurovatelných security ACL	1000	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO

Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	4000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, povýšením firmware	ANO, povýšením firmware
ISIS	ANO, povýšením firmware	ANO, povýšením firmware

IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	ANO, povýšením firmware
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, povýšením firmware	ANO, povýšením firmware
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (SSH, Syslog)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	ANO, povýšením firmware

IEEE 802.1ae na uplink portech	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO

Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO, povýšením firmware	ANO, povýšením firmware

Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE)	ANO	ANO
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požada	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_K1	Optický rozšiřující modul 10GE	min. 4x 10GE	C9200-NM-4X=	ANO
Modul_K2	Optický rozšiřující modul 1GE	min. 4x 1GE	C9200-NM-4G=	ANO
Modul_K3	Stohovací datový kabel	min. 1m	STACK-T4-1M=	ANO
Modul_K4	Stohovací datový kabel	min. 3m	STACK-T4-3M=	ANO
Modul_K5	Povýšení firmware o specifikované povýšitelné funkce	ANO	C9200-48-E-A-3	ANO

Požadavek na funkcionalitu	Minimální požadavk	Splňuje ANO/NE
Typ zařízení	Appliance pro automatizovaný dohled, správu a troubleshooting infrastruktury	DN2-HW-APL
Základní vlastnosti		
Formát zařízení	HW appliance	ANO
Vysoká dostupnost appliance v clusteru	ANO, cluster 3 uzlů	ANO
Možnost rozšíření o aplikaci automatizovaného dohledu, správy a troubleshootingu splňující následující vlastnosti: - Kompletní přehled stavu celé síťové infrastruktury v jednom pohledu - Detailní pohled na síťová zařízení, síťové služby i koncová zařízení - Správa životního cyklu síťových zařízení - Automatické discovery zařízení - Snadné vytváření politik (Intent-based, podle chodu organizace, nikoli použitých síťových technologií) - Zero-touch implementace síťových zařízení - Automatizované nasazení QoS - Segmentace infrastruktury do úrovně mikrosegmentace - Sběr analytických dat z každého zařízení v síti - Analýza skutečné příčiny síťových problémů a její dopřesnění na základě provozních a organizačních souvislostí (context based) - Návodný postup řešení detekovaných problémů - Retrospektivní analýza problémových situací klientů a infrastruktury - Grafický "traceroute" s detekcí problémů aplikací na mezilehlých uzlech - Otevřená API a SDK pro integraci s procesy organizace, s aplikacemi a systémy třetích stran	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Typ produktu	Wi-Fi Access Point pro vnitřní instalaci	C9120AXI-E
Základní vlastnosti		ANO
Způsob instalace AP	Strop/podhled	ANO
Typ antén	Integrované pro obě pásma	ANO
Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu	ANO	ANO
Samostatné rádio pro monitorování 2,4 a 5 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou síť, lokalizace klientů	ANO	ANO
Podpora standardů 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax)	ANO	ANO
Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	ANO	ANO
Minimální počet inzerovaných SSID (BSSID) per radio	8	ANO
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming)	ANO	ANO
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ANO	ANO
Access Pointy obsahují X.509 certifikát s lokální platností pro nasazení PKI	ANO	ANO
Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x suplikant	ANO	ANO
Podpora detekce a monitorování problémů WLAN odchyťáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ANO	ANO
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH	ANO	ANO
Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference)	ANO	ANO
Podpora rozpoznání zdroje rušivého signálu podle signatur	ANO	ANO
Access Point obsahuje radio podporující BLE 5.0, ZigBee, Thread a USB 2.0 port	ANO	ANO
1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz	ANO	ANO
Možnost 802.3af/at PoE napájení AP z přepínače nebo injectorů – plná funkce AP při použití 802.3at, v případě 802.3af AP běží minimálně v režimu 1x1 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu	ANO	ANO
AP uzavřené konstrukce bez větracích otvorů a ventilátoru	ANO	ANO
Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu	ANO	ANO
AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem.	ANO	ANO
Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům	ANO	ANO
Součástí dodávky každého AP jsou licence pro kontroler bezdrátové sítě a WLAN management.	ANO	ANO

Plná podpora AP na poptávaném kontroleru	ANO	ANO
--	-----	-----

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Typ produktu	Wi-Fi Access Point pro vnitřní instalaci	C9120AXE-E
Základní vlastnosti		ANO
Způsob instalace AP	Strop/podhled nebo stěna	ANO
Typ antén	Externí pro obě pásma	ANO
Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu	ANO	ANO
Samostatné rádio pro monitorování 2,4 a 5 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou síť, lokalizace klientů	ANO	ANO
Podpora standardů 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax)	ANO	ANO
Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	ANO	ANO
Minimální počet inzerovaných SSID (BSSID) per radio	8	ANO
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming)	ANO	ANO
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ANO	ANO
Access Pointy obsahují X.509 certifikát s lokální platností pro nasazení PKI	ANO	ANO
Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x suplikant	ANO	ANO
Podpora detekce a monitorování problémů WLAN odchyťáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ANO	ANO
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH	ANO	ANO
Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference)	ANO	ANO
Podpora rozpoznání zdroje rušivého signálu podle signatur	ANO	ANO
Access Point obsahuje radio podporující BLE 5.0, ZigBee, Thread a USB 2.0 port	ANO	ANO
1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz	ANO	ANO
Možnost 802.3af/at PoE napájení AP z přepínače nebo injectorů – plná funkce AP při použití 802.3at, v případě 802.3af AP běží minimálně v režimu 1x1 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu	ANO	ANO
AP uzavřené konstrukce bez větracích otvorů a ventilátoru	ANO	ANO
Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu	ANO	ANO
AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem.	ANO	ANO
Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům	ANO	ANO

Součástí dodávky každého AP jsou licence pro kontroler bezdrátové sítě a požadovaný WLAN management.	ANO	ANO
Plná podpora AP na požadovaném kontroleru	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_N1	Duální všesměrová anténa, 4 ks per AP	2 dBi@2,4 GHz, 4 dBi@5GHz	AIR-ANT2524DW-R	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ produktu	Kontroler bezdrátové sítě	C9800-40-K9
Formát kontroleru bezdrátové sítě	Fyzické zařízení, 1RU	ANO
Interní redundantní napájecí zdroj instalován	ANO	ANO
Minimální počet 1/10G SFP/SFP+ portů	4	ANO
Minimální propustnost pro data Gb/s	40	ANO
Požadované funkcionality kontroleru jsou licencovány dle počtu připojených AP, s granularitou 1 AP	ANO	ANO
Možnost upgradu až na 2000 registrovaných zalicencovaných AP	ANO	ANO
Minimální počet připojitelných klientů	32000	ANO
Redundance na úrovni kontrolerů a jejich portů, výpadek aktivního kontroleru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace)	ANO	ANO
Šifrovaná řídicí komunikace AP-kontroler	ANO	ANO
Možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost	ANO	ANO
Podpora mesh sítí, současné připojení normálních a mesh AP k jednomu kontroleru	ANO	ANO
Možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP	ANO	ANO
Podpora stávajících AP řady 2700, které má Zadavatel nasazeny ve své infrastruktuře	ANO	ANO
Bezpečnost a Guest Access		
Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování	ANO	ANO
Podpora RADIUS CoA	ANO	ANO
PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID	ANO	ANO
Podpora standardu „802.11w“ pro ochranu řídicích rámců na AP a klientovi	ANO	ANO
Integrované řešení návštěvnického přístupu s možností webové autentizace, bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP	ANO	ANO
Omezování počtu klientů per SSID	ANO	ANO
Lokální profilování zařízení – per uživatel a per zařízení	ANO	ANO
Detekce cizích AP a klientů, možnost vynuceného odpojení klientů od cizích AP	ANO	ANO

Podpora plného NetFlow v9 (RFC 3954) exportu záznamů o datových tocích uživatelů (vč. zdrojové a cílové IP adresy, portů, WLAN ID, počtu paketů a objemu přenesených dat) směrem k externímu kolektoru	ANO	ANO
Rychlý roaming		
Automatizované řešení roamingu uživatelů v rámci AP připojených na požadované i stávající kontrolery Zadavatele, L2/L3	ANO	ANO
Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP, možnost selektivního využití 802.11r na sdíleném SSID pouze pro zařízení, které tento standard podporují	ANO	ANO
Podpora standardu „802.11k“ pro optimalizaci roamingu	ANO	ANO
Podpora standardu „802.11v“ pro optimalizaci připojení klienta	ANO	ANO
QoS a řízení provozu v bezdrátové síti		
Podpora 802.11e/WMM	ANO	ANO
Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnanci a návštěvníci)	ANO	ANO
Mechanismy řízení přístupu (Call Admission Control) pro hasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma.	ANO	ANO
Podpora Video-streamingu se spolehlivým multicastem	ANO	ANO
Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	ANO	ANO
Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace	ANO	ANO
Správa frekvenčního pásma		
Automatizovaná centrální správa frekvenčního pásma	ANO	ANO
Monitoring rádiového spektra vč. 20/40/80/160 MHz kanálů, možnost okamžité automatické centralizovaně řízené reakce (změna kanálu nebo jeho šířky, změna vysílacího výkonu)	ANO	ANO
Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“)	ANO	ANO
Detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ANO	ANO
Troubleshooting rádiového signálu a automatické řešení problému rušivého signálu, generování alarmů na základě překročení prahových hodnot kvality signálu	ANO	ANO
Přiřazení tagů každému AP dle jeho umístění a účelu, konfigurace AP dle přiřazených tagů	ANO	ANO

Vytváření rádiových profilů (nastavení kanálů, rychlostí)	ANO	ANO
Dohled a správa kontroleru		
Centrální administrace správců s granularitou přístupových práv	ANO	ANO
Podpora správy přes serial CLI nebo přes IP pomocí SSH/telnet, http a https web GUI, SNMP	ANO	ANO
RJ45 konzolový port a/nebo USB konzolový port	ANO	ANO
Podpora API rozhraní pro dohled a plnou konfiguraci kontroleru pomocí NETCONF protokolu	ANO	ANO
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
Podpora Python scripting a Linux shell	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Aplikace softwarových záplat (bez potřeby povyšování celého firmware)	ANO	ANO
Automatický postupný upgrade jednotlivých AP dle jejich fyzického umístění	ANO	ANO
Lokalizační služby		
Pokročilé lokalizační služby zajištěny rozšířením kontroleru bezdrátové sítě (např. virtuální aplici)	ANO	ANO
Licence per aktivní AP	ANO	ANO
Lokalizace připojených klientů pomocí triangulace síly signálu	ANO	ANO
Lokalizace cizích AP a klientů pomocí triangulace síly signálu	ANO	ANO
Lokalizace a korelace zdrojů rušení bezdrátové sítě	ANO	ANO
Metriky/analytika chování připojených klientů	ANO	ANO
Podpora režimu vysoké dostupnosti pomocí více paralelně běžících instancí zařízení	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požadaví	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_O1	Licence pro připojení 1xAP k WiFi kontroleru včetně lokalizačních služeb	ANO	AIR-DNA	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Typ produktu	Aplikační platforma bezdrátové sítě (per AP)	DNAS-ACT
Základní vlastnosti		
Formát zařízení	Virtuální appliance a Cloud služba	ANO
Licence per aktivní AP	ANO	ANO
Lokalizace připojených klientů pomocí triangulace síly signálu	ANO	ANO
Lokalizace cizích AP a klientů pomocí triangulace síly signálu	ANO	ANO
Lokalizace a korelace zdrojů rušení bezdrátové sítě	ANO	ANO
Metriky/analytika chování připojených klientů	ANO	ANO
Funkce Hotspot webového portálu, vysoká škálovatelnost, zobrazení různých přihlašovacích portálů dle aktuální polohy klienta, možnost jazykových mutací, reporty a analytika, nástroje na vytváření stránek portálu	ANO	ANO
Rozšiřující funkce pro řešení individualizovaného obsahu pro konkrétní klienty, podpora SMS/email/API notifikací, dostupnost SDK pro vytvoření mobilní aplikace (Android, Apple)	ANO	ANO
REST API rozhraní pro získávání clientských dat	ANO	ANO
Funkce dohledového, řídicího a reportovacího nástroje lokalizovaných 802.11 WLAN klientů a RFID WLAN nebo BLE tagů, generování alermů nebo jiných událostí dle konfigurovatelných pravidel, možnost generování reportů	ANO	ANO
CLI rozhraní, SSHv2, dohled a konfigurace pomocí https web GUI	ANO	ANO
Podpora režimu vysoké dostupnosti pomocí více paralelně běžících instancí zařízení	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Architektura řešení	Spine-Leaf	N9K-C9332C
Řízení DC fabric infrastruktury	Prostřednictvím kontroleru	ANO
Redundance kontrolerů formou jejich zapojení do clusteru	ANO	ANO
Mód činnosti jednotlivých kontrolerů v clusteru	Všechny aktivní	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
IS-IS	ANO	ANO
BGPv4	ANO	ANO
BGPv6	ANO	ANO
802.1q	ANO	ANO
VXLAN enkapsulace	ANO	ANO
VXLAN bridging	ANO	ANO
VXLAN routing	ANO	ANO
IP multicast	ANO	ANO
DC fabric musí podporovat funkcionalitu distribuované default gateway na jednotlivých leaf přepínačích pro optimalizaci transportu aplikačního provozu	ANO	ANO
Integrace fyzických i virtuálních zařízení pro L4-L7 služby	ANO	ANO
DC fabric musí podporovat service-chaining: automatizované připojení a konfigurace zařízení pro L4-L7 služby	ANO	ANO
Integrace s hypervisorem VMware vSphere	ANO	ANO
Integrace s hypervisorem Microsoft Hyper-V	ANO	ANO
Integrace s Kubernetes prostředím	ANO	ANO
Plná integrace se zařízením Cisco FirePower	ANO	ANO
Congestion-aware load balancing datového provozu mezi jednotlivými DC fabric přepínači	ANO	ANO
Podpora vytváření multi-tenant prostředí	ANO	ANO
Podpora real time line rate telemetry (schopnost monitorovat každý paket, každý datový tok procházející DC fabric infrastrukturou)	ANO	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených geograficky distribuovanými clustery řídicích kontrolerů	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených společným clusterem s geograficky distribuovanými kontrolery	ANO	ANO
Spine přepínač pro DC fabric infrastrukturu		
Formát zařízení	Fixní	ANO
Redundantní AC zdroj (Port Side Intake airflow)	ANO	ANO
Celková propustnost přepínače	6,4 Tbps	ANO

Minimální počet neblokovaných portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	32	ANO
Podpora dual-rate 40/100GE QSFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
VXLAN enkapsulace	ANO	ANO
VXLAN routing	ANO	ANO
VXLAN with MP-BGP EVPN control plane	ANO	ANO
IEEE 802.3ad	ANO	ANO
Minimálně 8 linek jako součást LAG	ANO	ANO
Podpora "jumbo rámců"	Min. 9216 bytes	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	3900	ANO
Detekce protilehlého zařízení (např. LLDP)	ANO	ANO
Minimální počet host IPv4 routes	90000	ANO
OSPFv2, OSPFv3	ANO	ANO
IS-IS	ANO	ANO
BGP, MP-BGP	ANO	ANO
ECMP	ANO, min. 64 cest	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, min. 500	ANO
QoS - Priority Based Flow Control (IEEE 802.1Qbb)	ANO	ANO
QoS - Flow aware packet prioritization	ANO	ANO
QoS - Flowlet switching	ANO	ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
Line-rate šifrování prostřednictvím IEEE 802.1ae (AES-GCM-256)	ANO	ANO
Line-rate šifrování VXLAN paketů	ANO	ANO
Control Plane Policing nebo ekvivalentní funkcionality	ANO	ANO
Power-on autoprovisioning	ANO	ANO
CLI rozhraní	ANO	ANO
SSHv2	ANO	ANO
SNMPv3	ANO	ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
TACACS+ klient	ANO	ANO
Port mirroring (SPAN)	ANO	ANO
Vzdálený port mirroring přes L3 směrovanou síť	ANO	ANO
Syslog	ANO	ANO
Role Based Access Control	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Formát zařízení	Fixní	N9K-C93180YC-EX
Redundantní AC zdroj (front-to-back airflow)	ANO	ANO
Celková propustnost přepínače	3,6 Tbps	ANO
Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28	48	ANO
Minimální počet neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	6	ANO
Podpora dual-rate 40/100GE QSFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
Možnost volby protokolu na SFP portech: 1/10/25G Ethernet, 10G FCoE, 16/32G Fiber Channel	ANO	ANO
VXLAN routing	ANO	ANO
VXLAN with MP-BGP EVPN control plane	ANO	ANO
Podpora EVPN Route Type 2 (MAC/IP Advertisement Route), Route Type 3 (Inclusive Multicast Ethernet Tag Route), Route Type 4 (Ethernet Segment Route) a Route Type 5 (IP Prefix Route)	ANO	ANO
Policy based routing ve VXLAN infrastruktuře pro integraci L4-L7 zařízení	ANO	ANO
PVLAN ve VXLAN infrastruktuře	ANO	ANO
Možnost rozšířit funkcionalitu přepínače o IP multicast routing ve VXLAN infrastruktuře	ANO	ANO
VXLAN OAM - Ping	ANO	ANO
VXLAN OAM – Traceroute a Pathtrace	ANO	ANO
IEEE 802.3ad	ANO	ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)	ANO	ANO
Minimálně 32 linek jako součást Link Aggregation Group	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Groups	200	ANO
Podpora "jumbo rámců"	Min. 9216 bytes	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	3900	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Detekce protilehlého zařízení (např. LLDP)	ANO	ANO
Minimální počet MAC záznamů	70000	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS - Priority Based Flow Control (IEEE 802.1Qbb)	ANO	ANO
QoS - Flow aware congestion management	ANO	ANO
QoS - Flow aware packet prioritization	ANO	ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase	ANO	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	ANO
IEEE 802.1ae (AES-GCM-XPB-256) na všech SFP a QSFP portech	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
Minimální počet host IPv4 routes	200000	ANO
Minimální počet host IPv6 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
OSPFv2/OSPFv3	ANO	ANO
BGP/MP-BGP	ANO	ANO
IS-IS	ANO	ANO
ECMP	ANO, min. 64 cest	ANO
IGMPv2, IGMPv3	ANO	ANO
MLDv2	ANO	ANO
IGMP snooping	ANO	ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6	ANO	ANO
PIM BiDir	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
VRF Route Leaking	ANO	ANO
VRF Route Leaking pro IP Multicast	ANO	ANO
First Hop Redundancy Protokol pro IPv6	ANO	ANO
Port ACL, VLAN ACL	ANO	ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)	ANO	ANO
Line rate flow telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem)	ANO	ANO
Integrovaná Flow table	ANO, min. 32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Control Plane Policing	ANO	ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače	ANO	ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Model-driven telemetrie pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs apod.)	ANO	ANO
Model-driven telemetrie - gRPC/GRPC transport	ANO	ANO
Model-driven telemetrie – time-based a event-based triggers	ANO	ANO
Python scripting	ANO	ANO
Puppet, Chef, Ansible programming	ANO	ANO
Power-on autoprovisioning	ANO	ANO

CLI rozhraní	ANO	ANO
SSHv2	ANO	ANO
SNMPv3	ANO	ANO
TWAMP (RFC 5357) Reflector	ANO	ANO
NTP server	ANO	ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
TACACS+ klient	ANO	ANO
Port mirroring (SPAN)	ANO	ANO
Vzdálený port mirroring přes L3 směrovanou síť	ANO	ANO
Syslog	ANO	ANO
Role Based Access Control	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Architektura řešení	Spine-Leaf	N9K-C93240YC-FX2
Řízení DC fabric infrastruktury	Prostřednictvím kontroleru	ANO
Redundance kontrolerů formou jejich zapojení do clusteru	ANO	ANO
Mód činnosti jednotlivých kontrolerů v clusteru	Všechny aktivní	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
IS-IS	ANO	ANO
BGPv4	ANO	ANO
BGPv6	ANO	ANO
802.1q	ANO	ANO
VXLAN enkapsulace	ANO	ANO
VXLAN bridging	ANO	ANO
VXLAN routing	ANO	ANO
IP multicast	ANO	ANO
DC fabric musí podporovat funkcionalitu distribuované default gateway na jednotlivých leaf přepínačích pro optimalizaci transportu aplikačního provozu	ANO	ANO
Integrace fyzických i virtuálních zařízení pro L4-L7 služby	ANO	ANO
DC fabric musí podporovat service-chaining: automatizované připojení a konfigurace zařízení pro L4-L7 služby	ANO	ANO
Integrace s hypervisorem VMware vSphere	ANO	ANO
Integrace s hypervisorem Microsoft Hyper-V	ANO	ANO
Integrace s Kubernetes prostředím	ANO	ANO
Plná integrace se zařízením Cisco FirePower	ANO	ANO
Congestion-aware load balancing datového provozu mezi jednotlivými DC fabric přepínači	ANO	ANO
Podpora vytváření multi-tenant prostředí	ANO	ANO
Podpora real time line rate telemetry (schopnost monitorovat každý paket, každý datový tok procházející DC fabric infrastrukturou)	ANO	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených geograficky distribuovanými clustery řídicích kontrolerů	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených společným clusterem s geograficky distribuovanými kontrolery	ANO	ANO
Leaf přepínač pro DC fabric infrastrukturu		
Formát zařízení	Fixní	ANO
Redundantní AC zdroj (Port Side Intake airflow)	ANO	ANO
Celková propustnost přepínače	4,8 Tbps	ANO

Celový počet neblokovaných portů typu 1/10/25GE s volitelným fyzickým rozhraním typu SFP	48	ANO
Minimální počet neblokovaných portů 40/100GE s volitelným fyzickým rozhraním typu QSFP	12	ANO
Podpora dual-rate 40/100GE QSFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
VXLAN enkapsulace	ANO	ANO
VXLAN routing	ANO	ANO
IEEE 802.3ad	ANO	ANO
IEEE 802.3ad přes více šasi (Multichassis LAG)	ANO	ANO
Minimálně 8 linek jako součást LAG	ANO	ANO
Minimální počet konfigurovatelných LAGs	300	ANO
Podpora "jumbo rámců"	Min. 9216 bytes	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	3900	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Detekce protilehlého zařízení (např. LLDP)	ANO	ANO
QoS - Priority Based Flow Control (IEEE 802.1Qbb)	ANO	ANO
QoS - Flow aware packet prioritization	ANO	ANO
QoS - Flowlet switching	ANO	ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
Line-rate šifrování prostřednictvím IEEE 802.1ae (AES-GCM-256) na všech portech	ANO	ANO
Minimální počet host IPv4 routes	64000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
IS-IS	ANO	ANO
BGP, MP BGP	ANO	ANO
ECMP	ANO, min. 64 cest	ANO
IGMPv2, IGMPv3	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, min. 500	ANO
Control Plane Policing nebo ekvivalentní funkcionlita	ANO	ANO
Real time line rate telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem)	ANO	ANO
Integrovaná Flow table	ANO, min. 32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Power-on autoprovisioning	ANO	ANO
CLI rozhraní	ANO	ANO
SSHv2	ANO	ANO
SNMPv3	ANO	ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
TACACS+ klient	ANO	ANO

Port mirroring (SPAN)	ANO	ANO
Vzdálený port mirroring přes L3 směrovanou síť	ANO	ANO
Syslog	ANO	ANO
Role Based Access Control	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Formát zařízení	modulární	N77-C7706-B33S3E
Redundantní AC napájecí zdroj	ANO	ANO
Kapacita jednotlivého napájecího zdroje	min. 3000W	ANO
Možnost připojení napájecích zdrojů na dvě nezávislé rozvodné sítě	ANO	ANO
Minimální počet slotů v šasi pro instalaci ethernet modulů	4	ANO
Potenciální kapacita interní sběrnice na 1 slot přepínače	2,6 Tbps	ANO
Kapacita interní sběrnice na 1 slot přepínače v dodané konfiguraci	1,3 Tbps	ANO
Možnost instalovat redundantní řídicí modul	ANO	ANO
Podpora upgrade OS přepínače bez narušení provozu (In Service Software Upgrade)	ANO	ANO
Možnost rozdělit fyzické přepínač na několik logických přepínačů	ANO, min. 4	ANO
VXLAN bridging	ANO	ANO
VXLAN gateway	ANO	ANO
VXLAN routing	ANO	ANO
VXLAN with MP-BGP EVPN control plane	ANO	ANO
Policy based routing ve VXLAN infrastruktuře pro integraci L4-L7 zařízení	ANO	ANO
VXLAN OAM - Ping	ANO	ANO
VXLAN OAM – Traceroute a Pathtrace	ANO	ANO
IEEE 802.3ad	ANO	ANO
IEEE 802.3ad přes více šasi (Multichassis PortChannel)	ANO	ANO
Minimální počet konfigurovatelných PortChannel rozhraní	500	ANO
Minimálně 16 linek jako součást PortChannel rozhraní	ANO	ANO
Podpora "jumbo rámců"	Min. 9216 bytes	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	3900	ANO
IEEE 802.1ak	ANO	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO, min. 256	ANO
Detekce protilehlého zařízení (např. LLDP)	ANO	ANO
Minimální počet MAC záznamů	64000	ANO
Minimální počet IPv4 routes ve FIB	64000	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS Policing	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
OSPFv2	ANO	ANO
IS-IS	ANO	ANO
BGP	ANO	ANO

BGP 4-byte ASN	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
IP Multicast (PIM SM, PIM SSM)	ANO	ANO
IPv6 Multicast (PIM SM, PIM SSM)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
OSPFv3	ANO	ANO
MP BGP	ANO	ANO
VLAN ACL, Port ACL	ANO	ANO
Control Plane Policing	ANO	ANO
Podpora bezpečnostních funkcí umožňujících ochranu proti podvržení zdrojové IP adresy – IP source guard nebo ekvivalentní	ANO	ANO
Podpora bezpečnostních funkcí umožňujících ochranu proti připojení neautorizovaného DHCP serveru – DHCP snooping nebo ekvivalentní	ANO	ANO
Podpora bezpečnostních funkcí umožňujících inspekci provozu protokolu ARP – ARP inspection nebo ekvivalentní	ANO	ANO
CLI rozhraní	ANO	ANO
SSHv2	ANO	ANO
SNMPv3	ANO	ANO
NETCONF	ANO	ANO
Python programming	ANO	ANO
Puppet, Chef programming	ANO	ANO
NTP server	ANO	ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
TACACS+ klient	ANO	ANO
Port mirroring (SPAN)	ANO	ANO
Vzdálený port mirroring – ERSPAN nebo ekvivalentní	ANO	ANO
Syslog	ANO	ANO
Role Based Access Control	ANO	ANO
Podpora monitorování aplikačních toků s využitím NetFlow	ANO	ANO
Podpora exportu NetFlow dat dle formátu NetFlow v9 nebo IPFIX	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požadavky		Splňuje ANO/NE
	Základní vlastnosti			
Modul_T1	optický rozšiřující modul 100GE	min. 12x 100GE	N77-F312CK-26=	ANO
Modul_T2	optický rozšiřující modul 40GE	min. 24x 40GE	N77-F324FQ-25=	ANO
Modul_T3	optický rozšiřující modul 10GE	min. 48x 10GE	N77-F348XP-23=	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Architektura řešení	Spine-Leaf	APIC-M3
Řízení DC fabric infrastruktury	Prostřednictvím kontroleru	ANO
Redundance kontrolerů formou jejich zapojení do clusteru	ANO	ANO
Mód činnosti jednotlivých kontrolerů v clusteru	Všechny aktivní	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
IS-IS	ANO	ANO
BGPv4	ANO	ANO
BGPv6	ANO	ANO
802.1q	ANO	ANO
VXLAN enkapsulace	ANO	ANO
VXLAN bridging	ANO	ANO
VXLAN routing	ANO	ANO
IP multicast	ANO	ANO
DC fabric musí podporovat funkcionalitu distribuované default gateway na jednotlivých leaf přepínačích pro optimalizaci transportu aplikačního provozu	ANO	ANO
Integrace fyzických i virtuálních zařízení pro L4-L7 služby	ANO	ANO
DC fabric musí podporovat service-chaining; automatizované připojení a konfigurace zařízení pro L4-L7 služby	ANO	ANO
Integrace s hypervisorem VMware vSphere	ANO	ANO
Integrace s hypervisorem Microsoft Hyper-V	ANO	ANO
Integrace s Kubernetes prostředím	ANO	ANO
Plná integrace se zařízením Cisco FirePower	ANO	ANO
Congestion-aware load balancing datového provozu mezi jednotlivými DC fabric přepínači	ANO	ANO
Podpora vytváření multi-tenant prostředí	ANO	ANO
Podpora real time line rate telemetrie (schopnost monitorovat každý paket, každý datový tok procházející DC fabric infrastrukturou)	ANO	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených geograficky distribuovanými clusterly řídicích kontrolerů	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených společným clusterem s geograficky distribuovanými kontrolery	ANO	ANO
Požadovaná funkcionalita DC fabric kontroleru		
Škálovatelnost kontroleru - schopnost řídit DC fabric infrastrukturu s až 1200 přípojnými porty	ANO	ANO
Grafické uživatelské rozhraní součástí řešení	ANO	ANO
Přístupová práva založená na uživatelských rolích	ANO	ANO
Možnost rozdělit správu řešení mezi více vzájemně oddělených organizací (multitenantní řešení)	ANO	ANO

Funkce pro zcela automatické sestavení a konfiguraci fyzické infrastruktury DC fabric	ANO	ANO
Dokumentované API rozhraní pro volání všech dostupných funkcí řadiče, včetně těch, které jsou použity v grafickém uživatelském rozhraní	ANO	ANO
Možnost řízení aplikačních toků prostřednictvím definice aplikačních politik, které formou logického modelu popisují požadavky aplikací na síťovou konektivitu, bezpečnost, QoS a L4-L7 služby	ANO	ANO
Možnost členění fyzických a virtuálních serverů do logických skupin podle své funkce a na základě identifikátorů jako je IP adresa, MAC adresa, VLAN, VXLAN, VM name, VM OS type. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky (bezpečnostní požadavky, L4-L7 služby..) vůči jiným skupinám	ANO	ANO
Kontroler je centrálním místem pro definici aplikačních politik (bezpečnostní požadavky, L4-L7 služby..) jak pro fyzickou, tak i virtuální infrastrukturu DC fabric	ANO	ANO
GUI rozhraní pro detailní přehled o výkonnosti a stavu celé DC fabric infrastruktury včetně monitorování stavu jednotlivých DC přepínačů a aplikací	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Architektura řešení	Spine-Leaf	APIC-L3
Řízení DC fabric infrastruktury	Prostřednictvím kontroleru	ANO
Redundance kontrolerů formou jejich zapojení do clusteru	ANO	ANO
Mód činnosti jednotlivých kontrolerů v clusteru	Všechny aktivní	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
IS-IS	ANO	ANO
BGPv4	ANO	ANO
BGPv6	ANO	ANO
802.1q	ANO	ANO
VXLAN enkapsulace	ANO	ANO
VXLAN bridging	ANO	ANO
VXLAN routing	ANO	ANO
IP multicast	ANO	ANO
DC fabric musí podporovat funkcionalitu distribuované default gateway na jednotlivých leaf přepínačích pro optimalizaci transportu aplikačního provozu	ANO	ANO
Integrace fyzických i virtuálních zařízení pro L4-L7 služby	ANO	ANO
DC fabric musí podporovat service-chaining: automatizované připojení a konfigurace zařízení pro L4-L7 služby	ANO	ANO
Integrace s hypervisorem VMware vSphere	ANO	ANO
Integrace s hypervisorem Microsoft Hyper-V	ANO	ANO
Integrace s Kubernetes prostředím	ANO	ANO
Plná integrace se zařízením Cisco FirePower	ANO	ANO
Congestion-aware load balancing datového provozu mezi jednotlivými DC fabric přepínači	ANO	ANO
Podpora vytváření multi-tenant prostředí	ANO	ANO
Podpora real time line rate telemetry (schopnost monitorovat každý paket, každý datový tok procházející DC fabric infrastrukturou)	ANO	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených geograficky distribuovanými clustery řídicích kontrolerů	ANO	ANO
Možnost vzájemného propojení dvou DC fabric infrastruktur řízených společným clusterem s geograficky distribuovanými kontrolery	ANO	ANO
Požadovaná funkcionalita DC fabric kontroleru		
Škálovatelnost kontroleru - schopnost řídit DC fabric infrastrukturu s min. 1250 přípojnými porty	ANO	ANO
Grafické uživatelské rozhraní součástí řešení	ANO	ANO
Přístupová práva založená na uživatelských rolích	ANO	ANO

Možnost rozdělit správu řešení mezi více vzájemně oddělených organizací (multitenantní řešení)	ANO	ANO
Funkce pro zcela automatické sestavení a konfiguraci fyzické infrastruktury DC fabric	ANO	ANO
Dokumentované API rozhraní pro volání všech dostupných funkcí řadiče, včetně těch, které jsou použity v grafickém uživatelském rozhraní	ANO	ANO
Možnost řízení aplikačních toků prostřednictvím definice aplikačních politik, které formou logického modelu popisují požadavky aplikací na síťovou konektivitu, bezpečnost, QoS a L4-L7 služby	ANO	ANO
Možnost členění fyzických a virtuálních serverů do logických skupin podle své funkce a na základě identifikátorů jako je IP adresa, MAC adresa, VLAN, VXLAN, VM name, VM OS type. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky (bezpečnostní požadavky, L4-L7 služby..) vůči jiným skupinám	ANO	ANO
Kontroler je centrálním místem pro definici aplikačních politik (bezpečnostní požadavky, L4-L7 služby..) jak pro fyzickou, tak i virtuální infrastrukturu DC fabric	ANO	ANO
GUI rozhraní pro detailní přehled o výkonnosti a stavu celé DC fabric infrastruktury včetně monitorování stavu jednotlivých DC přepínačů a aplikací	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	firewall appliance	FPR4140-NGFW-K9
Výkon a funkcionalita firewallu		
Formát zařízení	Appliance, 1RU	Ano
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1	Ano
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	8	Ano
Možnost rozšíření o moduly rozhraní	2	Ano
Možnost rozšíření o další 10Gb SFP+ rozhraní	8	Ano
Možnost rozšíření o další 40Gb SFP+ rozhraní	4	Ano
Redundantní zdroje (Hot-Swappable)	;	Ano
Podporovaný počet současně otevřených spojení NGFW s AVC	25M	Ano
Rychlost vytváření nových spojení NGFW s AVC	160K	Ano
Propustnost stavového firewallu (multiprotokolový režim)	40 Gbps	Ano
Propustnost NGFW s AVC	25 Gbps	Ano
Propustnost NGFW s AVC, IPS	20 Gbps	Ano
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano	Ano
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	Ano
Podporovaný počet VLAN	Min. 1024	Ano
Vysoká dostupnost	Active/Active, Active/Standby	Ano
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano, až 16 boxů	Ano
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	Ano	Ano
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 7 kontextů	Ano	Ano
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	Ano
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	Ano
Podpora Policy based Routing	Ano	Ano
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	Ano
Podpora filtrace IPv4, IPv6	Ano	Ano
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	Ano
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	Ano

Podpora inspekce IPv6 provozu	Ano	Ano
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	Ano
Stateful inspekce minimálně těchto aplikačních protokolů: HTTP, FTP, Instant Messenger, File Sharing, SIP, H.323, SCCP, SMTP, ESMP, DNS, RPC, CIFS, MSRPC, NETBIOS	Ano	Ano
Podpora NAT64 a DNS64	Ano	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	Ano
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano	Ano
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	Ano
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	Ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	Ano
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	Ano
Výkon a funkcionality VPN funkcí firewall appliance		
Propustnost VPN koncentrátoru (šifrování 3DES/AES)	Min. 13 Gbps	Ano
Počet současných šifrovaných spojení	Min. 20000	Ano
Podpora IPsec VPN	Ano	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	Ano
Podpora nového protokolu pro výměny klíčů IKEv2	Ano	Ano
Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256	Ano	Ano
Podpora kontrolních mechanismů: MD5, SHA	Ano	Ano
Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256	Ano	Ano
Podpora komponentu Suite-B: SHA-2 mechanismu s metodami: SHA-256, SHA-384	Ano	Ano
Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA	Ano	Ano
Podpora SSL VPN	Ano	Ano
Podpora TLS i DTLS pro SSL připojení	Ano	Ano
Podpora SSL VPN v tunelovém režimu s distribucí VPN klientského SW přímo z FW	Ano	Ano

Podpora současné autentizace koncové stanice i uživatele	Ano	Ano
Podpora definice pravidel pro VPN přístup přímo prostředky FW a jejich automatická distribuce VPN připojeným klientům	Ano	Ano
Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů	Ano	Ano
Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)	Ano	Ano
Podpora definice různých LDAP nebo AD serverů podle mapování uživatelů na skupiny s využitím RADIUS, LDAP nebo hodnot v certifikátu	Ano	Ano
podpora VPN clustering a load balancing	Ano	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	Ano
Podpora veřejných CA, včetně možnosti CA přímo na firewallu	Ano	Ano
Možnost současné autentizace AAA a certifikátem	Ano	Ano
Možnost mapování některého DN pole certifikátu na uživatelskou identitu	Ano	Ano
Podpora CRL a OCSP pro kontrolu revokace certifikátu	Ano	Ano
Podpora SSO metod: KCD, Netegrity, ClearTrust, SAML, NTLM/FTP/CIFS pass-through, HTTP pass-through pomocí formuláře; HTTP-POST pomocí substitucí proměnných	Ano	Ano
Podpora IPv6 adresních rozsahů a přiřazení IPv6 adres klientům v případě dual-stack přístupu přes IPv4 infrastrukturu	Ano	Ano
Podpora čistého IPv6 přístupu na VPN koncentrátor	Ano	Ano
Možnost jednotné správy přístupu uživatelů přes VPN ale i lokálně na LAN a WiFi	Ano	Ano

Možnost rozšíření o základního VPN klienta následujících vlastností:	Ano	Ano
Jednotný klient pro IPsec (IKEv2) i SSL VPN	Ano	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	Ano
Funkce VPN pro vzdálené PC a mobilní platformy, včetně VPN pro jednotlivé aplikace na mobilních platformách, VPN pro IP phone a VPN klienty IKEv2 třetích stran	Ano	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	Ano

VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)	Ano	Ano
VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů	Ano	Ano
SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS.	Ano	Ano
VPN klient je lokalizován v českém jazyce	Ano	Ano

Možnost rozšíření o pokročilého VPN klienta následujících vlastností:	Ano	Ano
Podporuje šifrování nové generace, včetně algoritmů NSA Suite B - ESPv3 s IKEv2, 4096-bit RSA klíče, Diffie-Hellman group 24, a vylepšené SHA2 (SHA-256 a SHA-384)	Ano	Ano
Podporuje funkce prověření stavu koncového bodu pomocí definice vlastních pravidel založených na přítomnosti běžících procesů	Ano	Ano
Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačního systému	Ano	Ano

Možnost rozšíření o funkce NextGen FW (IPS, Antimalware ochrana, URL filtrace) následujících vlastností:	Ano	Ano
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	Ano
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano	Ano
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano	Ano
Možnost obejít IPS funkcí při zahlcení nebo nedostupnosti	Ano	Ano
Podpora 802.1Q tagovaných rámců	Ano	Ano
Inspekce pro IPv4 i IPv6	Ano	Ano
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano	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	Ano
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	Ano
Podpora aplikace pro psaní zákaznických filtrů	Ano	Ano
Podpora importu komunitních filtrů/signatur Snort	Ano	Ano
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	Ano

IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	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	Ano
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano	Ano
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	Ano
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano	Ano
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	Ano
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	Ano
Možnost definice uživatelské vrstvy politik	Ano	Ano
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano	Ano
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	Ano
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano	Ano
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano	Ano
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano	Ano
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano	Ano
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	Ano	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	Ano
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano	Ano
IPS musí být plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	Ano

Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	Ano
Možnost automatické i manuální klasifikace stanice jako „kritické“ se zohledněním v pravidlech, reportech apod.	Ano	Ano
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	Ano
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	Ano
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	Ano
Možnost definovat typ provozu předávaný k inspekci do Next-Gen FW	Ano	Ano
Podpora pasivního monitorování (TAP režim)	Ano	Ano
Možnost definovat režim provozu při zahlcení nebo nedostupnosti Next-Gen FW funkcí (fail open, fail close)	Ano	Ano
Možnost obejít Next-Gen FW funkcí při zahlcení nebo nedostupnosti	Ano	Ano
Podpora 802.1Q tagovaných rámců	Ano	Ano
Podpora virtuálních FW kontextů v Nex-Gen FW politikách	Ano	Ano
Podporovaných aplikací	Min. 3000	Ano
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	Ano
URL kategorií	80	Ano
Katagorizovaných světových URL	280 milionů	Ano
Rízení přístupu k WWW - Web Usage Control (WCU)	Ano	Ano
Filtrace podle typů aplikací webových i ne-webových	Ano	Ano
Filtrace podle reputace serverů	Ano	Ano
SSL inspekce (dekrypce/enkrypce)	Ano	Ano
Security Intelligence database – známé uzly botnet sítí C&C	Ano	Ano
Security Intelligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano	Ano
Možnost integrovat vlastní reputační databáze	Ano	Ano
Podpora komunitních, otevřených standardů popisu apliáci (OpenAppID)	Ano	Ano
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	Ano
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě (Network Behavior Analysis - NBA)	Ano	Ano
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení	Ano
	Operační systém	Ano
	Dodavatel OS	Ano
	Použité síť. protokoly	Ano
	Použité síť. služby	Ano
	Otevřené porty síť. služeb	Ano

	Potenciální zranitelnosti	Ano
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow	Ano
	Akce (allow, deny,..)	Ano
	Důvod případného blokování	Ano
	Zdroj. a cíl. adresa	Ano
	Vstupní a výstupní zóna	Ano
	Vstupní a výstupní rozhraní	Ano
	Zdroj. a cíl. port	Ano
	Aplikační protokol	Ano
	IPS událost, pokud vznikne	Ano
	Riziková úroveň IPS události	Ano
	Použitá síťová aplikace	Ano
	Rizikovost aplikace	Ano
	„Business impact“ aplikace	Ano
	Množství přenesených dat	Ano

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti				
Modul_W1	Optický rozšiřující modul 40GE	min. 4x 40GE	FPR4K-NM-4X40G=	FPR4K-NM-4X40G=	ANO
Modul_W2	Rozšíření o základního VPN klienta	min. 2500 uživatelů	L-AC-PLS-3Y-S6	L-AC-PLS-3Y-S6	ANO
Modul_W3	Rozšíření o pokročilého VPN klienta	min. 2500 uživatelů	L-AC-APX-3Y-S6	L-AC-APX-3Y-S6	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Appliance správy firewallů	FMC1600-K9
Centrální dohledová konzole ve formě HW platformi s podporou až 50 manažovatelných senzorů	Ano	Ano
Formát zařízení	Appliance, 1RU	Ano
Centrální dohledová konzole musí být schopna spracovat min. 30 milionů IPS událostí	Ano	Ano
Centrální dohledová konzole musí disponovat alespoň 32GB operační paměti	Ano	Ano
Centrální dohledová konzole musí disponovat procesorem Xeon 8-jader nebo výkonějším	Ano	Ano
Centrální dohledová konzole musí disponovat úložištěm min. 900GB	Ano	Ano
Podpora min. RAID 1	Ano	Ano
Síťová rozhraní min. 2x 1Gbps	Ano	Ano
Vzdálené správa konfigurace přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	Ano
Možnost správy přes příkazový řádek z lokální konzole a vzdáleným přístupem protokolem ssh	Ano	Ano
Možnost přístupu přes IPv6: SSHv2, Telnet, HTTP/HTTPS a ICMP	Ano	Ano
Možnost centrální správy při nasazení více firewallů	Ano	Ano
Při centrální správě: možnost sdílených bezpečnostních politik	Ano	Ano
Distribuce a správa SW firewallu, dalších modulů (např. pro VPN), konfigurací, licencí z grafického rozhraní managementu	Ano	Ano
Zobrazení logů a událostí v grafickém rozhraní správy s mapováním na konfiguraci bezpečnostních politik	Ano	Ano
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano	Ano
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	Ano
Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap	Ano	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	Ano
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	Ano
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	Ano

Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano	Ano
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	Ano
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano	Ano
Pro reporty lze definovat template definující formát a obsah reportu	Ano	Ano
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	Ano
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	Ano
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	Ano
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	Ano
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	Ano
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	Ano
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	Ano
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight	Ano
	BMC Remedy	Ano
	Trustwave	Ano
	NetForensics	Ano
	Novell Sentinel	Ano
	Hawk Network Defense	Ano
	Q1Labs-QRadar	Ano
	Log Rhythm SIEM 2.0	Ano
	LogLogic	Ano
	Splunk	Ano
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	Ano
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	Ano
Podpora řízeného přístupu podle rolí administrátorů	Ano	Ano
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	Ano
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano	Ano
Workflow pro předávání „ticketů“ mezi administrátory	Ano	Ano
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano	Ano

Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	Ano
Zákaznický definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano	Ano
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano	Ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	bezpečnostní brána pro Web provoz	WSA-S695F-K9
Appliance-based řešení s dedikovaným a optimalizovaným OS	2 RU	Ano
Alespoň 6 x 1Gb Ethernet rozhraní na HW platformě řešící webovou bezpečnost	Ano	Ano
Alespoň 2 x 10Gb Fiber rozhraní na platformě řešící webovou bezpečnost	Ano	Ano
Více pevných disků v hardwarovém poli RAID	RAID 10	Ano
Disková kapacita	9,6 TB	Ano
Hot-swap pevné disky	Ano	Ano
Více-jádrový CPU se SW podporou multi-core	2 x 2.6 Ghz, 12 jader	Ano
Kapacita paměti DRAM alespoň 64GB	Ano	Ano
Alespoň dva hot-swap napájecí zdroje	Ano	Ano
Podpora poskytovaná přímo od výrobce	Ano	Ano
Přístup na podporu dodavatele přes e-mail, telefon, web	Ano	Ano
Přístup na portál a znalostní databázi dodavatele	Ano	Ano
Kapacita HW zdrojů appliance pro ochranu alespoň 5000 uživatelů	Ano	Ano
Propustnost zařízení (počet HTTP transakcí za vteřinu), min 700/sec	Ano	Ano
Implementace transparentní proxy pomocí protokolu WCCPv2	Ano	Ano
Implementace transparentní proxy pomocí policy routing na L4 přepínači	Ano	Ano
Podpora explicitně definované proxy	Ano	Ano
Podpora implementace explicitní proxy pomocí PAC souborů a WPAD	Ano	Ano
Možnost hostování PAC souborů	Ano	Ano
Možnost více upstream proxy s conditional směrováním HTTP provozu	Ano	Ano
Více datových portů pro Web skenování	Ano	Ano
Podpora ochrany před Spyware/Adware/Generic Web threat	Ano	Ano
Ochrana před útoky typu Phishing	Ano	Ano
Automatický update pravidel pro ochranu před Phishing	Ano	Ano
Filtrování přístupu na webové stránky na základě kategorií	Ano	Ano
Zařízení obsahuje předdefinované kategorie	Ano	Ano
Možnost přidání vlastních kategorií webových stránek	Ano	Ano
Automatický update kategorií a jejich obsahu	Ano	Ano
Minimálně 60 podporovaných URL kategorií	Ano	Ano
Dynamická on-box kategorizace nezařazených URL	Ano	Ano
Dynamická cloud-based kategorizace nezařazených URL	Ano	Ano
Filtrování přístupu na webové stránky na základě reputace stránky	Ano	Ano
Nastavitelné prahy filtrace podle reputace na obsah: block/allow/scan	Ano	Ano
Filtrace na aplikační úrovni (AVC)	Ano	Ano

Podpora filtrace Web chat	Ano	Ano
Kontrola protokolů HTTP, HTTPS, FTP, Java, ActiveX	Ano	Ano
Filtrace Web elementů	Ano	Ano
Filtrace verzí prohlížeče	Ano	Ano
Detekce a analýza archivovaných (zazipovaných) souborů (i více archivů v sobě)	Ano	Ano
Detekce šifrovaných souborů a jejich případně blokování	Ano	Ano
Blokování podle maximální velikosti souboru	Ano	Ano
Podpora filtrace webmail	Ano	Ano
Blokování HTTP POST podle metadat	Ano	Ano
Skenování obsahu pro určení typu souboru	Ano	Ano
Kontrola provozu antivirovým systémem	Ano	Ano
Kontrola provozu antimalware systémem	Ano	Ano
Podpora filtrování podle reputace souborů	Ano	Ano
Podpora scanování příchozího i odchozího provozu	Ano	Ano
Monitorování L4 provozu s detekcí malwaru a blokováním „call-home“ provozu	Ano	Ano
Instalovaný antimalware software	Min.2 různé SW od dvou výrobců	Ano
Automatický update anti-malware signatur v 5-i minutových intervalech nebo menších	Ano	Ano
Nasazení jako transparentní proxy	Ano	Ano
Nasazení jako routed proxy	Ano	Ano
Blokování HTTP POST podle metadat	Ano	Ano
Skenování obsahu pro určení typu souboru	Ano	Ano
Ověření uživatele pomocí LDAP	Ano	Ano
Ověření uživatele pomocí NTLM	Ano	Ano
Přidělení skupinových politik podle LDAP/Active directory	Ano	Ano
Možnost definování „white/black“ listů	Ano	Ano
Politiky podle identity / zákazníka	Ano	Ano
Politiky definované podle časového rozsahu	Ano	Ano
Politiky definované podle kategorie	Ano	Ano
Politiky definované podle cílové URL	Ano	Ano
Politiky definované podle cílové IP adresy	Ano	Ano
HTTPS management konzole	Ano	Ano
CLI přístup pomocí SSH	Ano	Ano
RS232 sériové rozhraní	Ano	Ano
Možnosti centrálního managementu	Ano	Ano
Možnost zapnout pouze monitorování	Ano	Ano
Posílání informací / logování	Ano	Ano
Monitorování a blokování pokusů o nebezpečné spojení na všech 65535 TCP portech	Ano	Ano
Monitorování a blokování pokusů o nebezpečné spojení v obou směrech: vstupní i výstupní	Ano	Ano

Monitorování pomocí syslog	Ano	Ano
Monitorování pomocí SNMP	Ano	Ano
Monitorování pomocí XML	Ano	Ano
Centralizovaný management s více úrovní automatickou replikací konfigurací	Ano	Ano
Řízení uživatelské autentizace přes LDAP	Ano	Ano
Řízení uživatelské autentizace pomocí lokálních hesel	Ano	Ano
Možnosti read-only administrativních rolí	Ano	Ano
Možnost helpdesk uživatelské role s limitovanými oprávněními	Ano	Ano
Plný reporting přijímaných a odesílaných zpráv se širokými možnostmi vyhledávání	Ano	Ano
Monitorování pomocí syslog	Ano	Ano
Monitorování pomocí SNMP	Ano	Ano
Monitorování pomocí XML	Ano	Ano
Možnost rozšíření o pokročilou antimalware funkcionalitu následujících vlastností:	Ano	Ano
Řešení musí poskytovat rozšíření o pokročilou ochranu před malware, která rozšiřuje možnosti detekce a blokování antivirového softwaru o možnost blokování souborů na základe jejich reputace.	Ano	Ano
Rozšiřující pokročilá ochrana před malware musí umožňovat detekci a blokování škodlivého softwaru, poskytovat podrobné hlášení o chování souboru, průběžně analýzu souborů a výstrahy s retrospektivním verdiktem.	Ano	Ano
Řešení pokročilé ochrany před malware musí taky disponovat statickou a dynamickou analýzou souborů (sandboxing) a retrospekci výskytu souboru pro průběžnou analýzu hrozeb.	Ano	Ano

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_Y1	veškerá vyspecifikovaná ochrana Web provozu	min. 10000 uživatelů	WSA-WSP-LIC	ANO
Modul_Y2	rozšíření ochrany o pokročilou antimalware funkcionalitu	min. 10000 uživatelů	WSA-AMP-LIC	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	bezpečnostní brána pro Email provoz	ESA-C695F-K9
Appliance-based řešení s dedikovaným a optimalizovaným OS	2 RU	Ano
Alespoň 6 x 1Gb Ethernet rozhraní na platformě e-mail bezpečnosti	Ano	Ano
Alespoň 2 x 10Gb Fiber rozhraní na platformě e-mail bezpečnosti	Ano	Ano
Více pevných disků v hardware RAID poli	RAID 10	Ano
Disková kapacita	4,8 TB	Ano
Hot-swap pevné disky	Ano	Ano
Více-jádrový CPU s multicore SW podporou	1 x 2.6 GHz, 12 jader	Ano
Kapacita paměti DRAM alespoň 32GB	Ano	Ano
Alespoň dva hot-swap napájecí zdroje	Ano	Ano
Kapacita HW zdrojů appliance pro alespoň 10000 chráněných uživatelů	Ano	Ano
Podpora poskytovaná přímo od výrobce	Ano	Ano
Přístup na podporu dodavatele přes e-mail, telefon, web	Ano	Ano
Přístup na portál a znalostní databázi dodavatele	Ano	Ano
Podpora VLAN tagging	Ano	Ano
Podpora Ethernet NIC párování	Ano	Ano
Podpora plného real-time reportingu na boxu	Ano	Ano
Operátorská konzole pro tracking zpracování mailu	Ano	Ano
Ochrana operačního systému před přímým přístupem uživatele	Ano	Ano
Podpora pro RFC5321 SMTP	Ano	Ano
Podpora pro RFC3207 Secure SMTP over TLS	Ano	Ano
Podpora pro RFC4871 DKIM signing and verification	Ano	Ano
Podpora pro RFC4870 DomainKeys signing and verification	Ano	Ano
Podpora pro RFC4408 Sender Policy Framework verification	Ano	Ano
Podpora pro kontrolu certifikátů TLS	Ano	Ano
„False positives rate“ pro antis spam: 1 mail z 1 milionu nebo lepší	Ano	Ano
Používání reputační databáze při detekci spamů s defaultní „catch rate“ > 80%	Ano	Ano
Na základě hodnoty reputace musí být možné:	Ano	Ano
- odmítnout TCP spojení	Ano	Ano
- přijmout TCP spojení a odmítnout přijetí zprávy v rámci SMTP komunikace (SMTP reject)	Ano	Ano
- omezit počet zpráv přijatých od odesílatele	Ano	Ano
- vypnout skenování zpráv pro vabraného odesílatele	Ano	Ano
Podpora pro směrování zpráv s využitím LDAP	Ano	Ano
Podpora pro přepis adresy odesílatele a příjemce s pomocí LDAP	Ano	Ano

Verifikace příjemce v LDAP – zpráva pro neexistujícího příjemce musí být odmítnuta během SMTP komunikace bez toho, aby byl přijat obsah zprávy	Ano	Ano
Možnost přiřadit více IP adres pro každé rozhraní na emailové bráně	Ano	Ano
Podpora pro větší počet (>200) delivery rozhraní	Ano	Ano
Podpora pro možnost svázání specifického odchozího rozhraní pro konkrétního odesilatele nebo skupinu	Ano	Ano
Samostatné fronta pro každou destinaci elektronické pošty	Ano	Ano
Podpora pro separátní zpracování vstupních a výstupních emailů ve stejném čase	Ano	Ano
Per-message SMTP řízení	Ano	Ano
Limitace maximálního počtu současných spojení pro uživatele	Ano	Ano
Limitace maximálního počtu zpráv na spojení	Ano	Ano
Limitace maximálního počtu příjemců zprávy	Ano	Ano
Limitace maximálního počtu příjemců v čase	Ano	Ano
Podpora pro SMTP autentizaci	Ano	Ano
Podpora pro LDAP as SMTP autentizační backend	Ano	Ano
Podpora pro směrování SMTP autentizace	Ano	Ano
Podpora pro TLS enforcement pro SMTP autentizační požadavky	Ano	Ano
Ochrana před directory harvest útoky	Ano	Ano
Ochrana proti „bounce“spamům	Ano	Ano
Integrované (volitelné) šifrování jednotlivých zpráv	Ano	Ano
Možnost definování „white/black“ listů	Ano	Ano
Podpora pro anti-virus skenování s automatickými aktualizacemi signatur	Ano	Ano
Update anti-virus signatur minimálně každých 5 minut	Ano	Ano
Možnost vypnout/zapnout ativirus ochranu pro jednotlivé domény či uživatele	Ano	Ano
Možnost vypnout/zapnout antispam ochranu pro jednotlivé domény či uživatele	Ano	Ano
Reaktivní antispam a antivirus	Ano	Ano
Proaktivní antivirus (day zero outbreak filter nebo podobné řešení)	Ano	Ano
Podpora vícevrstvého antivirového řešení – možnost skenování zpráv více antivirovými softwary různých výrobců instalovanými na jedné emailové bráně	Ano	Ano
Podpora filtrování podle reputace souborů	Ano	Ano
Možnost přepisu URL (phishing) v těle mailu na URL mířící přes bezpečnostní web gateway	Ano	Ano
Integrace se systémem Domain Keys	Ano	Ano
Možnost přístupu do karantény pro jednotlivé uživatele	Ano	Ano
Možnost existence centrální karantény (v případě použití více fyzických zařízení)	Ano	Ano
Použití „appliance“ přístupu	Ano	Ano
Podpora managementu několika zařízení jako jednoho clusteru (včetně trackování zpráv)	Ano	Ano
Filtrování příloh na základě obsahu emailu (klíčová slova v těle emailu)	Ano	Ano
Filtrování příloh na základě přílohy (typ souboru)	Ano	Ano

Filtrování příloh na základě obsahu přílohy (klíčová slova v obsahu přílohy emailu, v PDF, XLS, DOC atp.)	Ano	Ano
Prevece virové nákazy (popř. neznámého typu spamu) na základě preventivních filtrů, založených na anomálním chování emailového provozu	Ano	Ano
HTTPS management konzole	Ano	Ano
CLI přístup pomocí SSH	Ano	Ano
RS232 sériové rozhraní	Ano	Ano
Centralizovaný management s více úroňovou automatickou replikací konfigurací	Ano	Ano
Řízení uživatelské autentizace přes LDAP	Ano	Ano
Řízení uživatelské autentizace pomocí lokálních hesel	Ano	Ano
Možnosti read-only administrativních rolí	Ano	Ano
Možnost helpdesk uživatelské role s limitovanými oprávněními	Ano	Ano
Plný reporting přijímaných a odesílaných zpráv se širokými možnostmi vyhledávání	Ano	Ano
Monitorování pomocí syslog	Ano	Ano
Monitorování pomocí SNMP	Ano	Ano
Monitorování pomocí XML	Ano	Ano
		Ano
Možnost rozšíření o pokročilou antimalware funkcionalitu následujících vlastností:		Ano
Řešení musí poskytovat rozšíření o pokročilou ochranu před malware, která rozšiřuje možnosti detekce a blokování antivirového softwaru o možnosti blokování souborů na základe jejich reputace.	Ano	Ano
Rozšiřující pokročilá ochrana před malware musí umožňovat detekci a blokování škodlivého softwaru, poskytovat podrobné hlášení o chování souboru, průběžnou analýzu souborů a výstrahy s retrospektivním verdiktem.	Ano	Ano
Řešení pokročilé ochrany před malware musí taky disponovat statickou a dynamickou analýzou souborů (sandboxing) a retrospekci výskytu souboru pro průběžnou analýzu hrozeb, a to i po průchodu e-mailovou branou.	Ano	Ano

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_Z1	veškerá vyspecifikovaná ochrana email provozu	min. 10000 mailboxů	ESA-ESP-LIC	ANO
Modul_Z2	rozšíření ochrany o pokročilou antimalware funkcionalitu	min. 10000 mailboxů	ESA-AMP-LIC	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Centralizovaná správa a reporting bran Email a Web bezpečnosti	SMA-M695F-K9
Appliance-based řešení s dedikovaným a optimalizovaným OS	2 RU	ano
Alespoň 6 x 1Gb Ethernet rozhraní na platformě e-mail bezpečnosti	ano	ano
Alespoň 2 x 10Gb Fiber rozhraní na platformě e-mail bezpečnosti	ano	ano
Více pevných disků v hardware RAID poli	RAID 10	ano
Disková kapacita	9,6 TB	ano
Hot-swap pevné disky	ano	ano
Více-jádrový CPU s multicore SW podporou	2 x 2.1 GHz, 8 jader	ano
Kapacita paměti DRAM alespoň 32GB	ano	ano
Alespoň dva hot-swap napájecí zdroje	ano	ano
Možnost jedné HW platformy pro centrální management/reporting/tracking Email i Web appliancí	ano	ano
Možnost centralizovaného sběru dat pro více e-mail bezpečnostních zařízení	ano	ano
Konsolidované reporty vytvořené z více dat a e-mail bezpečnostních zařízení	ano	ano
Rozhraní pro konsolidované tracking zpráv přes více e-mail bezpečnostních zařízení	ano	ano
Sběr karantény SPAMu z více e-mail bezpečnostních zařízení	ano	ano
Podpora přístupu koncového uživatele ke konsolidované karanténě SPAMu	ano	ano
Podpora pro uživatelskou autentizaci pomocí protokolu LDAP	ano	ano
Podpora pro uživatelskou autentizaci přes IMAP/POP autentizaci	ano	ano
Možnost informace (digest) o zařazení e-mailu do karantény pomocí e-mailu koncovým uživatelům	ano	ano
Podpora pro definování whitelist/blacklist koncovými uživateli	ano	ano
Podpora pro dodání digest přes relay	ano	ano
Podpora pro automatické informování o false-positive zprávách při jejich uvolnění z karantény	ano	ano
Možnost role Helpdesk s limitovanými možnostmi přístupu	ano	ano
HTTPS management konzole	ano	ano
CLI přístup pomocí SSH	ano	ano
RS232 sériové rozhraní	ano	ano
Možnost administrace uživatelských účtů s autentizací přes RADIUS	ano	ano
Administrace uživatelské autentizace pomocí lokálních hesel	ano	ano
Možnosti read-only administrativních rolí	ano	ano
Stateful záloha všech e-mail a web dat reportingu na druhém zařízení	ano	ano
Možnost naplánování zálohování dat	ano	ano

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_AA1	Rozšíření správy a reportingu Email brány o:	10000 uživatelů	SMA-EMGT-LIC	ANO
Modul_AA2	Rozšíření správy a reportingu Web brány o:	10000 uživatelů	SMA-WMGT-LIC	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	zařízení pro řízení identit a přístupu do sítě	L-ISE-BSE-PLIC
Obecná charakteristika ověřovacího řešení		
Centralizovaný systém pro ověřování uživatelů, 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, čas připojení apod.)	Ano	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 přístup	Ano	Ano
Poskytuje AAA funkce (viz níže)	Ano	Ano
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	Ano	Ano
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity	Ano	Ano
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	Ano	Ano
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)	Ano	Ano
Je dostupné ve formě Virtuálního stroje na platformách VMware ESXi, KVM a Microsoft Hyper-V	Ano	Ano
Počet obsluhovaných koncových klientů	100	Ano
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)		
Podporované protokoly		
RADIUS pro autentizaci, autorizaci, zaznamenávání	Ano	Ano
Proxy funkce pro externí RADIUS	Ano	Ano
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST	Ano	Ano
Možnost rozšíření o TACACS+ pro administraci zařízení	Ano	Ano
Podporované databáze uživatelů (s možností definovat pořadí průchodu)		
Interní (pro uživatele i koncová zařízení)	Ano	Ano
Active Directory	Ano	Ano
LDAP (RFC 2251)	Ano	Ano
RADIUS Token identity source (RFC 2865)	Ano	Ano
RSA RADIUS token server (OTP)	Ano	Ano
Open Database Connectivity (ODBC) a SAML	Ano	Ano
Certifikační autorita pro ověřování i autorizaci	Ano	Ano
Ověřování uživatelů a zařízení		

Ověření uživatelů heslem nebo certifikátem	Ano	Ano
Ověření MAC adresou připojovaného zařízení	Ano	Ano
Autorizace: pružný systém pro definici pravidel pro přístup k síti		
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:	Ano	Ano
· stavu a typu koncového zařízení (viz níže),	Ano	Ano
· uživatele (role, skupiny),	Ano	Ano
· místa připojení,	Ano	Ano
· historie připojení	Ano	Ano
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	Ano	Ano
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	Ano	Ano
Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“	Ano	Ano
Řízení přístupu i možným zapojením do trasy komunikace autorizovaných zařízení	Ano	Ano
Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů	Ano	Ano
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti	Ano	Ano
Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat	Ano	Ano
Accounting		
Zaznamenávání aktivity uživatelů a zařízení připojených k síti	Ano	Ano
Dotazovací systém, korelace záznamů, centralizované výkazy	Ano	Ano
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	Ano	Ano
Funkce GUEST serveru		
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi	Ano	Ano
Oprávnění přidělována správcem přístupu přes portál pro snadné vytváření dočasných účtů	Ano	Ano
Samoobslužný portál pro uživatele	Ano	Ano
Ověření přes HTTP a HTTPS	Ano	Ano
Další vlastnosti		
Možnost autentizace oproti více AD domén, i když nejsou v trust režimu	Ano	Ano
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	Ano	Ano
Podpora Multi-Domain integrace s AD	Ano	Ano
Podpora SXP (Exchange Protocol) dle IETF	Ano	Ano
Možnost rozšíření o rozpoznávání typu koncových zařízení následujících vlastností:		
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se sít'ovou infrastrukturou	Ano	Ano

Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)	Ano	Ano
Předdefinované profily pro síťová zařízení NAD od různých vendorů	Ano	Ano
Podpora pro IPv6 koncová zařízení	Ano	Ano
Možnost rozšíření o podporu BYOD následujících vlastností:		
Onboarding (registrace, provisioning, nastavení klientských zařízení)	Ano	Ano
Onboarding/provisioning proces formou samoobsluhu	Ano	Ano
Specifické politiky pro BYOD zařízení	Ano	Ano
Možnost nastavení limitu BYOD zařízení pro jednoho uživatele	Ano	Ano
Interní CA, pro vydávání certifikátů BYOD zařízením	Ano	Ano
Interní CA lze řetězit jako subordinate pod firemní CA	Ano	Ano
Možnost rozšíření o podporu MDM následujících vlastností:		
Workflow pro registrace do MDM	Ano	Ano
Výměna informací z MDM platformy a využití v politikách (např. pokud zařízení je „compliant“)	Ano	Ano
Ovládání MDM přímo z prostředků bezpečnostního managementu (zamykání, mazání, apod.) zařízení	Ano	Ano
Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení)	Ano	Ano
Možnost rozšíření o podporu rozpoznávání stavu koncových zařízení a jejich nápravu následujících vlastností:		
Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat:	Ano	Ano
· instalovaný operační systém (Windows 8.x (včetně Professional, Enterprise), Windows 7 (Professional, Ultimate, Enterprise, Home Premium, Home Basic, Starter edition), Windows Vista, Windows XP (Professional, Home, Media Center Edition, Tablet PC); Mac OS X v10.6.x a vyšší, Google Android 2.2 a vyšší, Apple iOS 5.0.1 a vyšší, Red Hat Enterprise Linux (RHEL) 5, Ubuntu)	Ano	Ano
· opravy instalované v operačním systému	Ano	Ano
· verze instalovaných programů	Ano	Ano
· hodnoty položek v registry databázi systémů Windows	Ano	Ano
· stav aplikací, zejména antivirů	Ano	Ano
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)	Ano	Ano
Funkce pro správu ověřovacího systému		
Centralizovaná správa	Ano	Ano
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	Ano	Ano
Zjednodušení správy vytváření skupin uživatelů, koncových a síťových zařízení	Ano	Ano
Grafické rozhraní pro definici pravidel přístupu k síti	Ano	Ano
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	Ano	Ano

Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	Ano	Ano
Zaznamenávání událostí na externí syslog server	Ano	Ano
Podpora SNMPv3	Ano	Ano
NTP pro synchronizaci času	Ano	Ano
SMTP pro zasílání zpráv a výstrah přes e-mail	Ano	Ano
Možnost provozování systému na aplici na následujících parametřích:		
Výpočetní výkon	Intel Xeon 2.10 GHz 4116, 12 jader	Ano
Operační paměť	96 GB	Ano
Úložný prostor	4x 600 GB 6Gb SAS 10K RPM	Ano
Dostupné komunikační rozhraní	6 x 1 GB	Ano
Podpora RAID	RAID 10	Ano
Síťová rozhraní	2x 10Gbase-T, 4x 1GBase-T	Ano

Komponent	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_AB1	Appliance pro provoz funkcionality řízení identit a přístupu do sítě	viz. specifikace prvku	SNS-3655-K9	ANO
Modul_AB2	Rozšíření řízení identit a přístupu do sítě o spravovaná koncová zařízení	min. 12000 koncových zařízení	L-ISE-BSE-P7	ANO
Modul_AB3	Rozšíření o funkcionalitu rozpoznávání typu koncových zařízení a BYOD	min. 10000 koncových zařízení	L-ISE-PLS-3Y-S7	ANO
Modul_AB4	Rozšíření o funkcionalitu rozpoznávání stavu koncových zařízení, jejich nápravy a MDM	min. 5000 koncových zařízení	L-ISE-APX-3Y-S6	ANO
Modul_AB5	Rozšíření o funkcionalitu TACACS+ pro administraci zařízení	ANO	L-ISE-TACACS-ND=	ANO

Požadavek na funkcionalitu	Minimální požadavk	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Klient pro ochranu koncové stanice	AMP4E-ADV-CL-LIC
Software na koncové stanici musí být menší než 100 MB a musí podporovat manuální a / nebo bezobslužnou instalaci	Ano	Ano
Software pro koncové stanice musí být snadno nasaditelný a musí podporovat (nejen) nasazení pomocí nástrojů pro správu systémů také 3. stran	Ano	Ano
Software musí být podporován na následujících platformách:		Ano
- Windows	Ano	Ano
- Mac	Ano	Ano
- Linux	Ano	Ano
- Android	Ano	Ano
- Virtuální zařízení	Ano	Ano
Analýza hlavní příčiny na podezřelých koncových stanicích musí poskytovat min. následující funkce:		Ano
- Sekvenční a chronologické stopy událostí s detaily, včetně hostitele, uživatelského jména, IP adresy a klientské aplikace	Ano	Ano
- Podrobnosti by měly zdůrazňovat, který soubor, proces, nebo služby byly ovlivněny	Ano	Ano
Navržený software pro koncové body musí podporovat sledování podezřelých souborů (malware) a poskytnout vizualizaci na úrovni sítě: postižené uživatele, systémy, Patient Zero – Day Zero (způsob a místo jakým hrozba pronikla do sítě)	Ano	Ano
Navrhovaný systém musí podporovat průběžné a neustálé monitorování souborů pro retrospektivní náhled detekce / blokování hrozby (malware)	Ano	Ano
Navrhovaný systém musí podporovat úplnou analýzu souborů v zabezpečené karanténě (sandbox) poskytující podrobnou zprávu o podezřelém chování souboru malware	Ano	Ano
Navrhovaný software pro koncové body musí být schopen blokovat CnC komunikaci, Sniffer/Dropper aktivity a obsah pro šíření škodlivého kódu	Ano	Ano
Reakce na událost a její náprava na koncových musí min. obsahovat:		Ano
- Sledování a zachytávání souborů s možností vyhledat škodlivé soubory na podezřelých koncových bodech	Ano	Ano
- Blokování souborů, procesů nebo služeb, které vykazují škodlivé chování	Ano	Ano
- Detekce Dropper aktivit a blokování stahování přes URL / web stránky	Ano	Ano
- Možnost odeslat podezřelé škodlivé soubory pro další analýzu	Ano	Ano

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
Modul_AD1	kabel 10GBASE-CU SFP+ 1 metr	1m	SFP-H10GB-CU1M	ANO
Modul_AD2	kabel 10GBASE-CU SFP+ 1,5 metru	1,5m	SFP-H10GB-CU1-5M	ANO
Modul_AD3	kabel 10GBASE-CU SFP+ 2 metry	2m	SFP-H10GB-CU2M	ANO
Modul_AD4	kabel 10GBASE-CU SFP+ 2,5 metru	2,5m	SFP-H10GB-CU2-5M	ANO
Modul_AD5	kabel 10GBASE-CU SFP+ 3 metry	3m	SFP-H10GB-CU3M	ANO
Modul_AD6	kabel 10GBASE-CU SFP+ 5 metrů	5m	SFP-H10GB-CU5M	ANO
Modul_AD7	kabel 10GBASE-CU SFP+ 7 metrů	7m	SFP-H10GB-ACU7M	ANO
Modul_AD8	kabel 10GBASE-CU SFP+ 10 metrů	10m	SFP-H10GB-ACU10M	ANO
Modul_AD9	10GBASE aktivní optický SFP+ kabel 1m	1m	SFP-10G-AOC1M	ANO
Modul_AD10	10GBASE aktivní optický SFP+ kabel 2m	2m	SFP-10G-AOC2M	ANO
Modul_AD11	10GBASE aktivní optický SFP+ kabel 3m	3m	SFP-10G-AOC3M	ANO
Modul_AD12	10GBASE aktivní optický SFP+ kabel 5m	5m	SFP-10G-AOC5M	ANO
Modul_AD13	10GBASE aktivní optický SFP+ kabel 7m	7m	SFP-10G-AOC7M	ANO
Modul_AD14	10GBASE aktivní optický SFP+ kabel 10m	10m	SFP-10G-AOC10M	ANO
Modul_AD15	10GBASE-SR SFP optický modul		SFP-10G-SR-S	ANO
Modul_AD16	10GBASE-LR SFP optický modul		SFP-10G-LR-S	ANO
Modul_AD17	10GBASE-LRM SFP optický modul		SFP-10G-LRM	ANO
Modul_AD18	10GBASE-ER SFP optický modul		SFP-10G-ER-S	ANO
Modul_AD19	10GBASE-ZR SFP optický modul		SFP-10G-ZR	ANO
Modul_AD20	Bidirectional SFP+ pro realizaci obousměrného spoje po 1 vlákne s dosahem 10km, downstream	downstream	SFP-10G-BXD-I	ANO
Modul_AD21	Bidirectional SFP+ pro realizaci obousměrného spoje po 1 vlákne s dosahem 10km, upstream	upstream	SFP-10G-BXU-I	ANO
Modul_AD22	1000BASE-T SFP optický modul		GLC-TE	ANO
Modul_AD23	1000BASE-SX SFP optický modul		GLC-SX-MMD	ANO
Modul_AD24	1000BASE-LX/LH SFP optický modul		GLC-LH-SMD	ANO
Modul_AD25	1000BASE-ZX SFP optický modul		GLC-ZX-SMD	ANO
Modul_AD26	40GE QSFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4		QSFP-40G-SR-BD	ANO
Modul_AD27	40GBASE-LR4 QSFP optický modul		QSFP-40G-LR4-S	ANO
Modul_AD28	kabel 40GBASE-CR4 QSFP pasivní metalický 1m	1m	QSFP-H40G-CU1M	ANO
Modul_AD29	kabel 40GBASE-CR4 QSFP pasivní metalický 3m	3m	QSFP-H40G-CU3M	ANO

Modul_AD30	kabel 40GBASE-CR4 QSFP pasivní metalický 5m	5m	QSFP-H40G-CU5M	ANO
Modul_AD31	kabel 40GBASE-CR4 QSFP aktivní metalický 7m	7m	QSFP-H40G-ACU7M	ANO
Modul_AD32	kabel 40GBASE-CR4 QSFP aktivní metalický 10m	10m	QSFP-H40G-ACU10M	ANO
Modul_AD33	kabel 40GBASE QSFP aktivní optický 1m	1m	QSFP-H40G-AOC1M	ANO
Modul_AD34	kabel 40GBASE QSFP aktivní optický 2m	2m	QSFP-H40G-AOC2M	ANO
Modul_AD35	kabel 40GBASE QSFP aktivní optický 3m	3m	QSFP-H40G-AOC3M	ANO
Modul_AD36	kabel 40GBASE QSFP aktivní optický 5m	5m	QSFP-H40G-AOC5M	ANO
Modul_AD37	kabel 40GBASE QSFP aktivní optický 7m	7m	QSFP-H40G-AOC7M	ANO
Modul_AD38	kabel 40GBASE QSFP aktivní optický 10m	10m	QSFP-H40G-AOC10M	ANO
Modul_AD39	kabel 40GBASE QSFP aktivní optický 15m	15m	QSFP-H40G-AOC15M	ANO
Modul_AD40	8 Gbit/s Fibre Channel Short Wave SFP+ optický modul		DS-SFP-FC8G-SW	ANO
Modul_AD41	8 Gbit/s Fibre Channel Long Wave SFP+ optický modul		DS-SFP-FC8G-LW	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Appliance pro podpůrné systémy	UCSC-C220-M5SX
Požadovaný formát zařízení	Rack mount	ANO
Maximální velikost	1 RU	ANO
Minimální počet instalovaných CPU	2	ANO
Minimální počet jader per instalované CPU	10	ANO
CINT 2006 Rates Baseline = 925 a vyšší	ANO	ANO
CFP 2006 Rates Baseline = 835 a vyšší	ANO	ANO
Paměť RAM o minimální velikosti 256 GB	ANO	ANO
Plně redundantní napájecí zdroje (plnohodnotná funkcionalita i s jedním zdrojem)	ANO	ANO
LOM síťový adaptér	ANO	ANO
Minimálně 2 porty 1/10GBASE-T na LOM síťovém adaptéru	ANO	ANO
mLOM CNA adaptér s možností vytváření virtuálních adaptérů typu vNIC a vHBA	ANO	ANO
Minimálně 4 porty 10/25GBASE SFP28 na mLOM síťovém adaptéru	ANO	ANO
Flash disk typu SD pro instalaci hypervizorů s kapacitou 64 GB a podporou zrcadlení SD karet pro vysokou dostupnost	ANO, min. 2	ANO
Možnost nahradit SD karty dvojicí SATA M.2 SSD	ANO	ANO
Minimálně 2 volné PCIe sloty pro rozšiřující adaptéry	ANO	ANO
Podpora IPMI (Intelligent Platform Management Interface) verze 2.0 technologie pro integraci managementu třetích stran	ANO	ANO
Možnost instalace CNA adaptéru s 2x40GE a s možností vytváření virtuálních adaptérů typu vNIC a vHBA		ANO
Možnost instalace deseti SFF SAS, SATA, nebo SSD disků pro lokální diskové úložiště vyměnitelných za provozu, z toho alespoň dva NVMe disky	ANO	ANO
Dedikovaný RAID řadič s minimálně 2GB cache, zálohovaný baterií	ANO	ANO
Podpora RAID 0, 1, 5, 6, 10, 50, 60 a JBOD režimu	ANO	ANO
Minimálně 2x pevný disk 1.2TB 12G SAS 10K RPM	ANO	ANO
Dedikovaný 1Gbps management port	ANO	ANO
HTML 5 GUI s virtuální KVM konzolí (HTML 5) pro vzdálený přístup v grafickém režimu s podporou mapování lokální či vzdálené ISO image.	ANO	ANO
Trusted Platform Module 2.0	ANO	ANO
Možnost povýšení operačního software zařízení a jednotlivých komponent po síti pomocí protokolů TFTP a HTTP přes lokální souborový systém	ANO	ANO
SNMPv2	ANO	ANO
SNMPv3	ANO	ANO
Syslog	ANO	ANO
Simple Mail Transfer Protocol (SMTP)	ANO	ANO
Key Management Interoperability Protocol (KMIP)	ANO	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Směrovač	ISR4331-SEC/K9
Formát zařízení	Modulární	ano
Požadovaný počet portů GigabitEthernet (WAN)	2x10/100/1000Base-TX, 1xSFP	ano
Sloty pro rozšiřující moduly	min. 3	ano
Dostupnost modulů s funkcionalitou akcelerace aplikací (CIFS, HTTP(S), MAPI, ICA ...) do směrovače	ano	ano
Dostupnost funkcionality akcelerace aplikací i v samotném firmware směrovače	ano	ano
Směrování IPv4	ano	ano
Směrování IPv6	ano	ano
OSPFv2	ano	ano
BGPv4	ano	ano
4 byte AS numbers in BGP	ano	ano
First Hop Redundancy Protokol (např. VRRP, HSRP)	ano	ano
GRE (Generic Routing Encapsulation)	ano	ano
Policy-based routing podle ACL	ano	ano
Přesměrování provozu na externí zařízení (WCCPv2)	ano	ano
Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830)	ano, povýšením firmware	ano, povýšením firmware
IP Multicast (PIM SSM, PIM SM)	ano	ano
IGMPv2, IGMPv3	ano	ano
uRPF	ano	ano
First Hop Redundancy Protokol pro IPv6	ano	ano
OSPFv3	ano	ano
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ano	ano
MP BGP	ano, povýšením firmware	ano, povýšením firmware
MPLS	ano, povýšením firmware	ano, povýšením firmware
MPLS VPN	ano, povýšením firmware	ano, povýšením firmware
EoMPLS	ano, povýšením firmware	ano, povýšením firmware
VPLS	ano, povýšením firmware	ano, povýšením firmware
Minimální počet oddělených (nezávislých) směrovacích tabulek	25	ano
IPv6 MPLS VPN (6VPE)	ano, povýšením firmware	ano, povýšením firmware
IPv6 Multicast (MLDv1 & v2)	ano	ano
IPv6 Multicast (PIM SM)	ano	ano
IPv6 Multicast (PIM SSM)	ano	ano

uRPF pro IPv6	ano	ano
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	ano	ano
QoS classification – ACL, DSCP, CoS, MPLS based	ano	ano
QoS marking - DSCP, CoS, MPLS	ano	ano
QoS Shaping	ano	ano
Class Based and Priority queuing	ano	ano
Rate Limiting	ano	ano
Hierarchical QoS	ano	ano
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, PING, traceroute)	ano, povýšením firmware	ano, povýšením firmware
ACL na rozhraní IN/OUT	ano	ano
IPSec AES 256	ano	ano
Minimální propustnost směrovače při aktivovaných službách IPSec šifrování a QoS měřená pro IMIX provoz	90Mb/s	ano
Směrovač lze doplnit na vyšší propustnost	ano, min. 250 Mb/s	ano
IKEv2	ano	ano
SHA-2 (SHA-256, SHA-512)	ano	ano
QoS pre-classification pro IPSec	ano	ano
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	ano	ano
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN, GET VPN) s centrální správou šifrovacích klíčů	ano	ano
Možnost rozšířit funkcionalitu směrovače o podporu technologie IEEE 802.1ae ve WAN prostředí	ano	ano
Zone based firewall	ano	ano
Stavová filtrace (firewall) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. Security Group Firewall nebo funkčně ekvivalentní)	ano	ano
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	ano
Monitorování aplikačních toků (za účelem detekce bezpečnostních incidentů) prostřednictvím technologie NetFlow nebo ekvivalentní	ano	ano

Definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód	ano	ano
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	ano	ano
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	ano	ano
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ano, povýšením firmware	ano, povýšením firmware
Směrování dle dynamicky měřených metrik, typu aplikace, zejména pro reálné a multimediální aplikace (např. Performance Routing nebo ekvivalentní)	ano, povýšením firmware	ano, povýšením firmware
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7.vrstvě OSI modelu dle aplikačních signatur)	ano, povýšením firmware	ano, povýšením firmware
Rozšiřování signatur rozpoznávaných aplikací bez přerušení provozu	ano, povýšením firmware	ano, povýšením firmware
Kategorizace rozpoznávaných aplikací	ano, povýšením firmware	ano, povýšením firmware
Vynucení QoS parametrů pro takto rozpoznávané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	ano, povýšením firmware	ano, povýšením firmware
Měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků (využívané pásmo, odezvy, RTP statistiky, počty aplikačních spojení ...)	ano, povýšením firmware	ano, povýšením firmware
Export a reporting rozpoznávaných aplikací a jejich statistik a výkonnostních charakteristik pomocí NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano, povýšením firmware	ano, povýšením firmware
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS, bez nutnosti dešifrování paketů	ano	ano
Ochrana proti narušení modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ano	ano
Podpora Secure Unique Device Identity (IEEE 802.1AR) pro ověření autentičnosti HW prostředků zařízení	ano	ano

SSHv2	ano	ano
CLI rozhraní	ano	ano
Programovatelnost prostřednictvím NETCONF/YANG	ano	ano
Python scripting	ano	ano
Model-driven telemetry pro real-time streaming informací o stavu zařízení	ano	ano
SNMPv2/v3	ano	ano
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	ano
NTPv3 server	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Vlastnost směrovače	UCS-E160S-M3/K9=_1
Typické pozicování zařízení	pobočka	ano
Formát zařízení	vlastnost směrovače	ano
Minimální velikost disku	200GB SSD	ano
Minimální velikost paměti	16GB RAM směrovače	ano
Minimální velikost FLASH paměti	16GB	ano
Minimální počet optimalizovaných TCP spojení	750	ano
Požadavky na redukci přenášených dat		
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN.	ano	ano
Obsah dočasně uložených dat na disku musí být šifrovaný standardem FIPS 140-2 level 2, 256-bit AES.	ano	ano
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávání, tak aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache.	ano	ano
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, tak aby docházelo k přenášení změn a ne celých souborů.	ano	ano
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	ano	ano
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování).	ano	ano
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall.	ano	ano
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních.	ano	ano
Vlastnosti akcelerace TCP/IP		
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	ano	ano
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390.	ano	ano
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	ano	ano
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů).	ano	ano
Vlastnosti akcelerace CIFS		
		ano

Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata jako jsou atributy souborů nebo adresářová struktura.	ano	ano
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele.	ano	ano
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetěžené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching).	ano	ano
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows, jako například v Microsoft Active directory.	ano	ano
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS.	ano	ano
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů.	ano	ano
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení.	ano	ano
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení.	ano	ano
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel.	ano	ano
Vlastnosti akcelerace aplikací		ano
Akcelerační zařízení musí podporovat akceleraci HTTP	ano	ano
Akcelerační zařízení musí podporovat akceleraci SSL	ano	ano
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	ano	ano
Akcelerační zařízení musí podporovat akceleraci CIFS	ano	ano
Možnost rozšíření o využívání Internetových content distribution nebo content caching služeb (např. Akamai)	ano	ano
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	ano	ano
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	ano	ano
Zařízení musí podporovat licencovanou akceleraci MAPI	ano	ano
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	ano	ano
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci.	ano	ano
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	ano	ano
Microsoft SMS: podpora akcelerace SMS.	ano	ano
Akcelerační zařízení musí podporovat akceleraci SMBv2	ano	ano
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	ano	ano
Akcelerační zařízení musí podporovat přednačítání obsahu pro SharePoint	ano	ano
Možnost rozšíření o caching HTTP videa (live i on-demand, HLS, HDS, HSS, YouTube)	ano	ano
Management		ano
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem.	ano	ano

Řešení musí poskytnout nástroje na odstraňování problémů.	ano	ano
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG.	ano	ano
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou.	ano	ano
Autentizace správců pomocí RADIUS nebo LDAP.	ano	ano
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC).	ano	ano
Řešení musí podporovat SNMPv3	ano	ano
System musí zajistit detailní rozpoznání a klasifikaci přenášených aplikací (Deep Packet Inspection)	ano	ano
System musí zajistit vynucování politik dle detailního rozpoznání aplikací	ano	ano
Komunikace managementu a akceleračních zařízení musí být zabezpečena/šifrovaná.	ano	ano
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https.	ano	ano
Sběr a prezentace dat výkonnosti aplikací ze vzdálených lokalit v centrálním managementu	ano	ano
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	ano	ano
Export dat pomocí protokolu NetFlow v9 a IPFIX	ano	ano
Možnosti implementace		ano
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty.	ano	ano
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	ano	ano
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky.	ano	ano
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace.	ano	ano
Řešení s daným zařízením musí umožňovat rozšiřování kapacity WAN optimalizace bez jejího přerušení	ano	ano
Řešení s daným zařízením musí umožňovat flexibilní a elastické rozšiřování - kombinace fyzických WAN optimalizátorů i virtuálních optimalizátorů (běžící v prostředí Vmware a pod.) do jedné sady/skupiny	ano	ano
Řešení s daným zařízením musí umožňovat automatické rovnoměrné rozkládání zátěže mezi optimalizátory v dané skupině	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině podle jejich aktuálního vytížení	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině, nebo mezi skupiny optimalizátorů dle konfigurovatelných politik, dle jednotlivých vzdálených poboček, dle přenášených aplikací či v případě vzájemného zálohování	ano	ano
Řešení s daným zařízením musí umožňovat stavová redundance jednotlivých aplikačních spojení	ano	ano

Řešení s daným zařízením musí umožňovat optimalizace i v případě asymetrických datových toků, asymetrického směrování i mezi geograficky oddělenými lokalitami	ano	ano
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu samostatné appliance	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení tvořeném vlastním směrovačem bez přídatných modulů	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMWare	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	zařízení pro akceleraci aplikací ve WAN	UCS-E160S-M3/K9=_2
Typické pozicování zařízení	pobočka	ano
Formát zařízení	univerzální modul do směrovače	ano
Minimální velikost disku	1TB	ano
Minimální počet CPU jader	6	ano
Minimální velikost paměti	16 GB	ano
Minimální počet optimalizovaných TCP spojení	750	ano
Požadavky na redukci přenášených dat		
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN.	ano	ano
Obsah dočasně uložených dat na disku musí být šifrovaný standardem FIPS 140-2 level 2, 256-bit AES.	ano	ano
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávání, tak aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache.	ano	ano
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, tak aby docházelo k přenášení změn a ne celých souborů.	ano	ano
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	ano	ano
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování).	ano	ano
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall.	ano	ano
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních.	ano	ano
Vlastnosti akcelerace TCP/IP		
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	ano	ano
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390.	ano	ano
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	ano	ano

Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů).	ano	ano
Vlastnosti akcelerace CIFS		ano
Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata jako jsou atributy souborů nebo adresářová struktura.	ano	ano
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele.	ano	ano
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetězené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching).	ano	ano
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows, jako například v Microsoft Active directory.	ano	ano
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS.	ano	ano
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů.	ano	ano
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení.	ano	ano
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení.	ano	ano
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel.	ano	ano
Vlastnosti akcelerace aplikací		ano
Akcelerační zařízení musí podporovat akceleraci HTTP	ano	ano
Akcelerační zařízení musí podporovat akceleraci SSL	ano	ano
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	ano	ano
Akcelerační zařízení musí podporovat akceleraci CIFS	ano	ano
Možnost rozšíření o využívání Internetových content distribution nebo content caching služeb (např. Akamai)	ano	ano
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	ano	ano
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	ano	ano
Zařízení musí podporovat licencovanou akceleraci MAPI	ano	ano
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	ano	ano
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci.	ano	ano
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	ano	ano
Microsoft SMS: podpora akcelerace SMS.	ano	ano
Akcelerační zařízení musí podporovat akceleraci SMBv2	ano	ano
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	ano	ano

Akcelerační zařízení musí podporovat přednačítání obsahu pro SharePoint	ano	ano
Možnost rozšíření o caching HTTP videa (live i on-demand, HLS, HDS, HSS, YouTube)	ano	ano
Management		ano
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem.	ano	ano
Řešení musí poskytnout nástroje na odstraňování problémů.	ano	ano
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG.	ano	ano
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou.	ano	ano
Autentizace správců pomocí RADIUS nebo LDAP.	ano	ano
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC).	ano	ano
Řešení musí podporovat SNMPv3	ano	ano
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná.	ano	ano
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https.	ano	ano
System musí zajistit detailní rozpoznání a klasifikaci přenášených aplikací (Deep Packet Inspection)	ano	ano
System musí zajistit vynucování politik dle detailního rozpoznání aplikací	ano	ano
Sběr a prezentace dat výkonosti aplikací ze vzdálených lokalit v centrálním managementu	ano	ano
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	ano	ano
Export dat pomocí protokolu NetFlow v9 a IPFIX	ano	ano
Možnosti implementace		ano
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty.	ano	ano
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	ano	ano
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky.	ano	ano
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace.	ano	ano
Řešení s daným zařízením musí umožňovat rozšiřování kapacity WAN optimalizace bez jejího přerušení	ano	ano
Řešení s daným zařízením musí umožňovat flexibilní a elastické rozšiřování - kombinace fyzických WAN optimalizátorů i virtuálních optimalizátorů (běžící v prostředí Vmware a pod.) do jedné sady/skupiny	ano	ano
Řešení s daným zařízením musí umožňovat automatické rovnoměrné rozkládání zátěže mezi optimalizátory v dané skupině	ano	ano

Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině podle jejich aktuálního vytížení	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině, nebo mezi skupiny optimalizátorů dle konfigurovatelných politik, dle jednotlivých vzdálených poboček, dle přenášených aplikací či v případě vzájemného zálohování	ano	ano
Řešení s daným zařízením musí umožňovat stavovou redundanci jednotlivých aplikačních spojení	ano	ano
Řešení s daným zařízením musí umožňovat optimalizaci i v případě asymetrických datových toků, asymetrického směřování i mezi geograficky oddělenými lokalitami	ano	ano
Jedno zařízení musí být schopno akceleroovat provoz ve více VRF současně se zachováním oddělení provozu a překryvnými adresními prostory	ano	ano
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	ano	ano
Zařízení musí akceleroovat i proti "peer" zařízení, které je ve formátu samostatné appliance	ano	ano
Zařízení musí akceleroovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	ano	ano
Zařízení musí akceleroovat i proti "peer" zařízení tvořeném vlastním směrovačem bez přídatných modulů	ano	ano
Zařízení musí akceleroovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMWare	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Zařízení pro akceleraci aplikací ve WAN	UCS-E160S-M3/K9=_3
Typické pozicování zařízení	pobočka	ano
Formát zařízení	univerzální modul do směrovače	ano
Minimální velikost disku	1TB	ano
Minimální počet CPU jader	6	ano
Minimální velikost paměti	16GB	ano
Minimální počet optimalizovaných TCP spojení	1300	ano
Požadavky na redukci přenášených dat		
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN.	ano	ano
Obsah dočasně uložených dat na disku musí být šifrovaný standardem FIPS 140-2 level 2, 256-bit AES.	ano	ano
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávání, tak aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache.	ano	ano
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, tak aby docházelo k přenášení změn a ne celých souborů.	ano	ano
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	ano	ano
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování).	ano	ano
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall.	ano	ano
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních.	ano	ano
Vlastnosti akcelerace TCP/IP		
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	ano	ano
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390.	ano	ano
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	ano	ano
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů).	ano	ano
Vlastnosti akcelerace CIFS		

Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata jako jsou atributy souborů nebo adresářová struktura.	ano	ano
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele.	ano	ano
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetěžené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching).	ano	ano
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows, jako například v Microsoft Active directory.	ano	ano
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS.	ano	ano
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů.	ano	ano
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení.	ano	ano
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení.	ano	ano
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel.	ano	ano
Vlastnosti akcelerace aplikací		
Akcelerační zařízení musí podporovat akceleraci HTTP	ano	ano
Akcelerační zařízení musí podporovat akceleraci SSL	ano	ano
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	ano	ano
Akcelerační zařízení musí podporovat akceleraci CIFS	ano	ano
Možnost rozšíření o využívání Internetových content distribution nebo content caching služeb (např. Akamai)	ano	ano
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	ano	ano
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	ano	ano
Zařízení musí podporovat licencovanou akceleraci MAPI	ano	ano
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	ano	ano
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci.	ano	ano
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	ano	ano
Microsoft SMS: podpora akcelerace SMS.	ano	ano
Akcelerační zařízení musí podporovat akceleraci SMBv2	ano	ano
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	ano	ano
Akcelerační zařízení musí podporovat přednačítání obsahu pro SharePoint	ano	ano
Možnost rozšíření o caching HTTP videa (live i on-demand, HLS, HDS, HSS, YouTube)	ano	ano
Management		
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem.	ano	ano

Řešení musí poskytnout nástroje na odstraňování problémů.	ano	ano
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG.	ano	ano
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou.	ano	ano
Autentizace správců pomocí RADIUS nebo LDAP.	ano	ano
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC).	ano	ano
Řešení musí podporovat SNMPv3	ano	ano
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná.	ano	ano
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https.	ano	ano
System musí zajistit detailní rozpoznání a klasifikaci přenášených aplikací (Deep Packet Inspection)	ano	ano
System musí zajistit vynucování politik dle detailního rozpoznání aplikací	ano	ano
Sběr a prezentace dat výkonnosti aplikací ze vzdálených lokalit v centrálním managementu	ano	ano
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	ano	ano
Export dat pomocí protokolu NetFlow v9 a IPFIX	ano	ano
Možnosti implementace		
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty.	ano	ano
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	ano	ano
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky.	ano	ano
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace.	ano	ano
Řešení s daným zařízením musí umožňovat rozšiřování kapacity WAN optimalizace bez jejího přerušení	ano	ano
Řešení s daným zařízením musí umožňovat flexibilní a elastické rozšiřování - kombinace fyzických WAN optimalizátorů i virtuálních optimalizátorů (běžící v prostředí Vmware a pod.) do jedné sady/skupiny	ano	ano
Řešení s daným zařízením musí umožňovat automatické rovnoměrné rozkládání zátěže mezi optimalizátory v dané skupině	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině podle jejich aktuálního vytížení	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině, nebo mezi skupiny optimalizátorů dle konfigurovatelných politik, dle jednotlivých vzdálených poboček, dle přenášených aplikací či v případě vzájemného zálohování	ano	ano
Řešení s daným zařízením musí umožňovat stavovou redundanci jednotlivých aplikačních spojení	ano	ano
Řešení s daným zařízením musí umožňovat optimalizaci i v případě asymetrických datových toků, asymetrického směrování i mezi geograficky oddělenými lokalitami	ano	ano

Jedno zařízení musí být schopno akcelerovat provoz ve více VRF současně se zachováním oddělení provozu a překryvnými adresními prostory	ano	ano
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu samostatné appliance	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení tvořeném vlastním směrovačem bez přídavných modulů	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMWare	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Zařízení pro akceleraci aplikací ve WAN	UCS-E160S-M3/K9=_4
Typické pozicování zařízení	pobočka	ano
Formát zařízení	univerzální modul do směrovače	ano
Minimální velikost disku	1TB	ano
Minimální počet CPU jader	6	ano
Minimální velikost paměti	32GB	ano
Minimální počet optimalizovaných TCP spojení	2500	ano
Požadavky na redukci přenášených dat		ano
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN.	ano	ano
Obsah dočasně uložených dat na disku musí být šifrován standardem FIPS 140-2 level 2, 256-bit AES.	ano	ano
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávání, tak aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache.	ano	ano
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, tak aby docházelo k přenášení změn a ne celých souborů.	ano	ano
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	ano	ano
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování).	ano	ano
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall.	ano	ano
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních.	ano	ano
Vlastnosti akcelerace TCP/IP		ano
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	ano	ano
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390.	ano	ano
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	ano	ano
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů).	ano	ano
Vlastnosti akcelerace CIFS		ano
Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata jako jsou atributy souborů nebo adresářová struktura.	ano	ano
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele.	ano	ano
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvídání výpočetních operací, multiplexing datových přenosů, zřetěžené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching).	ano	ano

Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows, jako například v Microsoft Active directory.	ano	ano
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS.	ano	ano
Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů.	ano	ano
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení.	ano	ano
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení.	ano	ano
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel.	ano	ano
Vlastnosti akcelerace aplikací		ano
Akcelerační zařízení musí podporovat akceleraci HTTP	ano	ano
Akcelerační zařízení musí podporovat akceleraci SSL	ano	ano
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	ano	ano
Akcelerační zařízení musí podporovat akceleraci CIFS	ano	ano
Možnost rozšíření o využívání Internetových content distribution nebo content caching služeb (např. Akamai)	ano	ano
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	ano	ano
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	ano	ano
Zařízení musí podporovat licencovanou akceleraci MAPI	ano	ano
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	ano	ano
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci.	ano	ano
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	ano	ano
Microsoft SMS: podpora akcelerace SMS.	ano	ano
Akcelerační zařízení musí podporovat akceleraci SMBv2	ano	ano
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	ano	ano
Akcelerační zařízení musí podporovat přednačítání obsahu pro SharePoint	ano	ano
Možnost rozšíření o caching HTTP videa (live i on-demand, HLS, HDS, HSS, YouTube)	ano	ano
Management		ano
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem.	ano	ano
Řešení musí poskytnout nástroje na odstraňování problémů.	ano	ano
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG.	ano	ano
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou.	ano	ano
Autentizace správců pomocí RADIUS nebo LDAP.	ano	ano
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC).	ano	ano
Řešení musí podporovat SNMPv3	ano	ano
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná.	ano	ano
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https.	ano	ano
System musí zajistit detailní rozpoznání a klasifikaci přenášených aplikací (Deep Packet Inspection)	ano	ano
System musí zajistit vynucování politik dle detailního rozpoznání aplikací	ano	ano

Sběr a prezentace dat výkonností aplikací ze vzdálených lokalit v centrálním managementu	ano	ano
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	ano	ano
Export dat pomocí protokolu NetFlow v9 a IPFIX	ano	ano
Možnosti implementace		ano
Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty.	ano	ano
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	ano	ano
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky.	ano	ano
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace.	ano	ano
Řešení s daným zařízením musí umožňovat rozšiřování kapacity WAN optimalizace bez jejího přerušení	ano	ano
Řešení s daným zařízením musí umožňovat flexibilní a elastické rozšiřování - kombinace fyzických WAN optimalizátorů i virtuálních optimalizátorů (běžící v prostředí Vmware a pod.) do jedné sady/skupiny	ano	ano
Řešení s daným zařízením musí umožňovat automatické rovnoměrné rozkládání zátěže mezi optimalizátory v dané skupině	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině podle jejich aktuálního vytížení	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině, nebo mezi skupiny optimalizátorů dle konfigurovatelných politik, dle jednotlivých vzdálených poboček, dle přenášených aplikací či v případě vzájemného zálohování	ano	ano
Řešení s daným zařízením musí umožňovat stavovou redundanci jednotlivých aplikačních spojení	ano	ano
Řešení s daným zařízením musí umožňovat optimalizaci i v případě asymetrických datových toků, asymetrického směrování i mezi geograficky oddělenými lokalitami	ano	ano
Jedno zařízení musí být schopno akcelerovat provoz ve více VRF současně se zachováním oddělení provozu a překryvnými adresními prostory	ano	ano
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu samostatné appliance	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení tvořeném vlastním směrovačem bez přídatných modulů	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMWare	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	Zařízení pro akceleraci	UCS-E160S-M3/K9=_5
Typické pozicování zařízení	pobočka	ano
Formát zařízení	univerzální modul do směrovače	ano
Minimální velikost disku	1TB	ano
Minimální počet CPU jader	6	ano
Minimální velikost paměti	32GB	ano
Minimální počet optimalizovaných TCP spojení	6000	ano
Požadavky na redukci přenášených dat		
Zařízení musí poskytnout cachovací techniky na pevném disku pro redukci přenášených dat po WAN.	ano	ano
Obsah dočasně uložených dat na disku musí být šifrovaný standardem FIPS 140-2 level 2, 256-bit AES.	ano	ano
Zařízení musí dovolit vzorkování binárních dat a jejich zpětné rozeznávání, tak aby bylo možné přenášet změny provedené v souborech a obnovení zbytku obsahu ze vzorků v cache.	ano	ano
Zařízení musí disponovat kompresí na úrovni bytů, ne na úrovni souborů, tak aby docházelo k přenášení změn a ne celých souborů.	ano	ano
Zařízení musí přizpůsobit ukládání vzorků binárních dat (šetřit kapacitu cache) primárnímu směru toku dat jednotlivých aplikací (např. při virtualizaci desktopů)	ano	ano
Zařízení musí využívat uložených vzorků v centrálním zařízení pro více vzdálených lokalit (šetřit kapacitu cache, zvýšit škálování).	ano	ano
Řešení musí být transparentní pro síťovou infrastrukturu (zachovávat klíčové informace o datových tocích) a neovlivňovat chování nástrojů závislých na informacích v TCP/IP záhlaví, zejména s ohledem na technologie netflow, QoS, firewall.	ano	ano
Řešení musí podporovat možnost zachování ToS/DSCP QoS značky na optimalizovaných spojeních.	ano	ano
Vlastnosti akcelerace TCP/IP		
TCP akcelerace (libovolná metoda změny velikosti okna, selektivní potvrzování nebo kombinace) může být použita jedině v případě zachování datové integrity	ano	ano
Pro TCP akceleraci musí být použito doporučení ze standardů RFC 1323, RFC 2018, RFC 3390.	ano	ano
TCP akcelerace musí být transparentní, tj. zachovávat IP a TCP údaje obsažené v hlavičce paketu (zdrojové a cílové IP adresy, čísla TCP portů, QoS)	ano	ano
Akcelerační zařízení musí být schopno přizpůsobit WAN optimalizaci chování linky (latence, ztrátovost paketů).	ano	ano
Vlastnosti akcelerace CIFS		
Akcelerační zařízení musí poskytnout lokálně metadata CIFS a být schopno dočasně uchovat caching-metadata jako jsou atributy souborů nebo adresářová struktura.	ano	ano
Akcelerační zařízení musí poskytnout lokální úložiště pro pobočkové uživatele.	ano	ano
Funkce pro zrychlení protokolu a minimalizaci aplikačního zpoždění, včetně načítání aplikací v předstihu, předvidání výpočetních operací, multiplexing datových přenosů, zřetěžené zpracování dat (pipelining) a dávkové zpracování výpočetních operací (operation batching).	ano	ano
Nevyžaduje žádné změny v autentifikačních či autorizačních konfiguracích Windows, jako například v Microsoft Active directory.	ano	ano
Plná podpora autentifikace systémů Windows NT LAN Manager a Kerberos pro žádosti v protokolu CIFS.	ano	ano

Nikdy si nepřivlastňuje vzorovou kopii souboru nebo datového prvku ani stav zamykání souborů.	ano	ano
Plně zachovává a dodržuje sémantiku protokolu, chrání soudržnost dat a směrodatnou kopii musí vždy vlastnit výchozí zařízení.	ano	ano
Centralizovaně řízená distribuce dat a služba přednačítání obsahu, tedy možnost centrálně přesouvat soubory do pobočkových zařízení.	ano	ano
Možnost přístupu k souboru i při výpadku konektivity WAN dle definovaných pravidel.	ano	ano
Vlastnosti akcelerace aplikací		ano
Akcelerační zařízení musí podporovat akceleraci HTTP	ano	ano
Akcelerační zařízení musí podporovat akceleraci SSL	ano	ano
Akcelerační zařízení musí podporovat přechod z optimalizovaného HTTP na optimalizované SSL během navazování spojení	ano	ano
Akcelerační zařízení musí podporovat akceleraci CIFS	ano	ano
Možnost rozšíření o využívání Internetových content distribution nebo content caching služeb (např. Akamai)	ano	ano
Akcelerační zařízení musí podporovat ověřování platnost certifikátů (např. OSCP protokol)	ano	ano
Akcelerační zařízení musí podporovat ověřování pomocí klientských i serverových certifikátů	ano	ano
Zařízení musí podporovat licencovanou akceleraci MAPI	ano	ano
Zařízení musí podporovat licencovanou akceleraci Encrypted MAPI	ano	ano
Zařízení musí dovolovat škálování pro nové aplikace bez požadavků na rekonfiguraci.	ano	ano
Print Services: zařízení musí podporovat akceleraci tiskových služeb pro pobočkový a centrální tisk včetně distribuce/managementu tiskových driverů	ano	ano
Microsoft SMS: podpora akcelerace SMS.	ano	ano
Akcelerační zařízení musí podporovat akceleraci SMBv2	ano	ano
Akcelerační zařízení musí podporovat akceleraci ICA, včetně ICA over SSL	ano	ano
Akcelerační zařízení musí podporovat přednačítání obsahu pro SharePoint	ano	ano
Možnost rozšíření o caching HTTP videa (live i on-demand, HLS, HDS, HSS, YouTube)	ano	ano
Management		ano
Řešení musí dovolit kompletní centrální správu všech akceleračních zařízení centrálním managementem.	ano	ano
Řešení musí poskytnout nástroje na odstraňování problémů.	ano	ano
Řešení musí poskytnout nástroje pro odeslání upozornění pomocí SNMP TRAP, SMTP nebo SYSLOG.	ano	ano
Management musí být možné konfigurovat jako redundantní do geograficky oddělených datových center s L3 konektivitou.	ano	ano
Autentizace správců pomocí RADIUS nebo LDAP.	ano	ano
Řešení může umožnit nastavení rolí pro jednotlivé správce a skupiny správců (RBAC).	ano	ano
Řešení musí podporovat SNMPv3	ano	ano
Komunikace managementu a akceleračních zařízení musí být zabezpečená/šifrovaná.	ano	ano
Přístup správců k lokálnímu managementu akceleračních zařízení musí být zabezpečen/šifrován metodami ssh, https.	ano	ano
Systém musí zajistit detailní rozpoznání a klasifikaci přenášených aplikací (Deep Packet Inspection)	ano	ano
Systém musí zajistit vynucování politik dle detailního rozpoznání aplikací	ano	ano
Sběr a prezentace dat výkoností aplikací ze vzdálených lokalit v centrálním managementu	ano	ano
Řešení musí umožnit automatickou instalaci a konfiguraci vzdáleného akceleračního zařízení	ano	ano
Export dat pomocí protokolu NetFlow v9 a IPFIX	ano	ano
Možnosti implementace		ano

Zařízení musí dovolit flexibilní nasazení mimo cestu (WCCP, PBR) a/nebo nasazení transparentně přímo do cesty.	ano	ano
Zařízení musí umožňovat dynamickou formaci dvojic odpovědných za akceleraci a de-akceleraci toků (peer autodiscovery)	ano	ano
Řešení s daným zařízením musí podporovat load-sharing přes několik akceleračních zařízení v případě, že jedno nedovede obsloužit všechny požadavky.	ano	ano
Řešení s daným zařízením musí podporovat redundantní WAN linky a asymetrické směrování v infrastruktuře při zachování akcelerace.	ano	ano
Řešení s daným zařízením musí umožňovat rozšiřování kapacity WAN optimalizace bez jejího přerušování	ano	ano
Řešení s daným zařízením musí umožňovat flexibilní a elastické rozšiřování - kombinace fyzických WAN optimalizátorů i virtuálních optimalizátorů (běžící v prostředí Vmware a pod.) do jedné sady/skupiny	ano	ano
Řešení s daným zařízením musí umožňovat automatické rovnoměrné rozkládání zátěže mezi optimalizátory v dané skupině	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině podle jejich aktuálního vytížení	ano	ano
Řešení s daným zařízením musí umožňovat automatické rozkládání zátěže mezi optimalizátory v dané skupině, nebo mezi skupiny optimalizátorů dle konfigurovatelných politik, dle jednotlivých vzdálených poboček, dle přenášených aplikací či v případě vzájemného zálohování	ano	ano
Řešení s daným zařízením musí umožňovat stavovou redundanci jednotlivých aplikačních spojení	ano	ano
Řešení s daným zařízením musí umožňovat optimalizaci i v případě asymetrických datových toků, asymetrického směrování i mezi geograficky oddělenými lokalitami	ano	ano
Jedno zařízení musí být schopno akcelerovat provoz ve více VRF současně se zachováním oddělení provozu a překryvnými adresními prostory	ano	ano
Automatické vyhledávání a identifikace „peer“ akceleračních zařízení pro in-line i off-path implementace	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu samostatné appliance	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu modulu do směrovače	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení tvořeném vlastním směrovačem bez přídavných modulů	ano	ano
Zařízení musí akcelerovat i proti "peer" zařízení, které je ve formátu virtuálního zařízení v VMWare	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	směrovač	ASR1001-X
Formát zařízení	Modulární	ano
Oddělený procesor pro funkce směrování a forwardování paketů	ano	ano
Minimální počet portů GigabitEthernet SFP	6	ano
Redundantní zdroj	ano	ano
Minimální počet slotů pro moduly v chassis	2	ano
Možnost budoucího povýšení nabídnutých portů na technologii 10GE (min. 2 porty)	ano	ano
Možnost softwarové redundance routovacího procesu	ano	ano
Směrování IPv4	ano	ano
Směrování IPv6	ano	ano
Možnost rozšíření o funkci NAT mezi IPv4 a IPv6	ano	ano
Výkonnostní parametry		
Minimální propustnost forwardovacího procesoru	19 Mpps	ano
Minimální kombinovaná propustnost forwardovacího procesoru při zapnutých funkcích QoS, ACL, RPF	6 Mpps	ano
Minimální dostupná kapacita šasi	5 Gbps	ano
Kapacita povyšována licenčně, bez povyšování HW	Ano	ano
Maximální dosažitelná kapacita bez povýšení HW	min. 20 Gbps	ano
Minimální kapacita šifrování v HW (IMIX, AES256)	5 Gbps	ano
Minimální propustnost Firewall	5 Gbps	ano
Minimální propustnost NAT pro IPv4	5 Gbps	ano
Počet záznamů ve směrovací tabulce - IPv4 Unicast	min. 1 000 000	ano
Počet záznamů ve směrovací tabulce – IPv6 Unicast	min. 500 000	ano
Minimální počet oddělených (nezávislých) směrovacích tabulek (např. VRF nebo ekvivalentní)	50	ano
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	ano
Podpora IEEE 802.3ad	ano	ano
Podpora "jumbo rámců"	ano	ano
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	ano
QoS classification – ACL, DSCP, CoS based	ano	ano
QoS marking - DSCP, CoS	ano	ano
QoS Shaping and Policing	ano	ano
Class Based and Priority queuing	ano	ano
Rate Limiting	ano	ano

Hierarchický QoS	3 úrovně, 16 000 front	ano
RSVP	ano	ano
DSCP-based Queue Mapping	ano	ano
DHCP relay	ano	ano
Router redundancy protokol (např. VRRP, HSRP)	ano	ano
Transport Ethernet rámců přes L3 páteř (např. OTV nebo EVI nebo funkčně ekvivalentní)	ano	ano
uRPF	ano	ano
IPv6		
First Hop Redundancy Protokol pro IPv6	ano	ano
MP BGP	ano	ano
IPv6 Multicast (MLDv1 & v2)	ano	ano
IPv6 Multicast (PIM SM)	ano	ano
IPv6 Multicast (PIM SSM)	ano	ano
IPv6 SLA nebo ekvivalentní technologie	ano	ano
uRPF pro IPv6	ano	ano
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	ano	ano
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie	ano	ano
DHCPv6 Relay	ano	ano
MPLS		
Label Imposition a Label Disposition (MPLS Provider Edge)	ano	ano
Label Swapping (MPLS Provider Core)	ano	ano
LDP (Label Distribution Protocol)	ano	ano
MPLS VPN	ano	ano
QoS s využitím MPLS EXP bitů	ano	ano
EoMPLS	ano	ano
VPLS	ano	ano
Směrovací protokoly		
BGPv4	ano	ano
Podpora 4 byte AS numbers in BGP	ano	ano
OSPFv2, OSPFv3	ano	ano
OSPF s MD5 a NSSA	ano	ano
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ano	ano
RIPv2	ano	ano
Policy-based routing podle ACL	ano	ano
Směrování multicastu		
PIM (dense i sparse mód)	ano	ano
IGMPv2 a IGMPv3	ano	ano
IPv6 MLDv1 & v2 snooping	ano	ano

Bezpečnost		
Podpora reverse path check (uRPF)	ano	ano
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.1ad)	ano	ano
ACL pro IP	ano	ano
ACL pro ethernetové rámce	ano	ano
Zone-based Stavový firewall	ano	ano
IPSec VPN	ano	ano
Dynamické sestavování IPSec VPN tunelů pro automatické vytvoření full-mesh topologie	ano	ano
IPSec VPN bez potřeby vytvářet tunely (GET VPN)	ano	ano
NSA Suite-B šifrovací algoritmy	ano	ano
IPSec AES 256 v hardware	ano	ano
IKEv2	ano	ano
SHA-2 (SHA-256, SHA-512)	ano	ano
Podpora klasifikace bezpečnostní role přístupujícího uživatele nebo koncového zařízení a její propagace sítě (např. Security Group Exchange Protocol dle RFC draft-smith-kandula-sxp-01 nebo funkčně ekvivalentní).	ano	ano
Podpora propagace bezpečnostní role uživatele nebo koncového zařízení pro každý datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní)	ano	ano
Podpora hardwarové filtrace (stavová filtrace, firewall) podle bezpečnostních rolí uživatelů propagovaných sítí přístupujících k různým skupinám síťových prostředků (např. Security Group Firewall, nebo funkčně ekvivalentní)	ano	ano
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ano	ano
Podpora přenosu aplikací		
Možnost rozšíření o pokročilou detekci a klasifikaci jednotlivých přenášených aplikací (DPI na 7.vrstvě OSI modelu dle aplikačních signatur)	ano	ano
Možnost doplnění o rozšiřování signatur rozpoznávaných aplikací bez přerušení provozu	ano	ano
Možnost doplnění o kategorizaci rozpoznávaných aplikací	ano	ano
Možnost rozšíření o Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	ano	ano
Možnost rozšíření o měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - využívané pásmo	ano	ano
Možnost rozšíření o měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - odezvy aplikací	ano	ano
Možnost rozšíření o měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - RTP statistiky	ano	ano
Možnost rozšíření o měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - počty aplikačních spojení	ano	ano

Možnost rozšíření o export a reporting rozpoznávaných aplikací a jejich statistik a výkonnostních charakteristik pomocí NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	ano
Management		
CLI rozhraní a SSHv2	ano	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ano
SNMPv2	ano	ano
SNMPv3	ano	ano
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ano	ano
Čítače paketů pro jednotlivá pravidla v ACL	ano	ano
Sériová konzolová linka	ano	ano
DNS klient	ano	ano
NTP klient s MD5 autentizací	ano	ano
Administrátorem definovatelné monitory (sady statistik) sbírané o každém přenášeném paketu	ano	ano
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)	ano	ano
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano	ano
Statistiky exportovatelné pomocí NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	ano
Možnost rozšíření o export detekované aplikace již daný "flow" náleží	ano	ano
Nástroje pro měření dynamických parametrů a odezev v síti v libovolný okamžik, synteticky generovaným provozem (například IP SLA nebo ekvivalentní)	ano	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	ano
TACACS+ klient	ano	ano
Syslog	ano	ano
Model-driven telemetry pro real-time streaming informací o stavu zařízení	ano	ano
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloADERu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchors	ano	ano
Podpora SUDI (IEEE 802.1AR) autentizace	ano	ano
Programovatelnost prostřednictvím NETCONF/YANG	ano	ano
Python scripting	ano	ano
Služby		
NTP server	ano	ano
DHCP server	ano	ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Požadavek na funkcionalitu		
Typ zařízení	Směrovač	ASR1002-HX
Formát zařízení	Modulární	ANO
Redundantní AC napájecí zdroj (interní)	ANO	ANO
Požadovaný počet portů 10 GigabitEthernet s volitelným fyzickým rozhraním	4	ANO
Požadovaná rozšiřitelnost na min. 8 portů 10 GigabitEthernet s volitelným fyzickým rozhraním	ANO	ANO
Požadovaný počet portů 1 GigabitEthernet s volitelným fyzickým rozhraním	4	ANO
Požadovaná rozšiřitelnost na min. 8 portů 1 GigabitEthernet s volitelným fyzickým rozhraním	ANO	ANO
Požadovaná rozšiřitelnost na min. 2 porty 40 GigabitEthernet s volitelným fyzickým rozhraním	ANO	ANO
Oddělený procesor pro funkce směrování a forwardování paketů	ANO	ANO
Směrování IPv4	ANO	ANO
Směrování IPv6	ANO	ANO
Propustnost systému	100Gb/s	ANO
Paketový výkon směrovače	56Mpps	ANO
Minimální počet záznamů ve směrovací tabulce - IPv4	3,5M	ANO
Minimální počet záznamů ve směrovací tabulce – IPv6	3M	ANO
IEEE 802.3ad	ANO	ANO
OSPFv2	ANO	ANO
BGPv4	ANO	ANO
Podpora 4 byte AS numbers in BGP	ANO	ANO
Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
GRE (Generic Routing Encapsulation)	ANO	ANO
Policy-based routing podle ACL	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
uRPF	ANO	ANO
DHCP relay	ANO	ANO
First Hop Redundancy Protokol pro IPv6	ANO	ANO
OSPFv3	ANO	ANO
MP BGP	ANO	ANO

IPv6 Multicast (MLDv1 & v2)	ANO	ANO
IPv6 Multicast (PIM SM)	ANO	ANO
IPv6 Multicast (PIM SSM)	ANO	ANO
IPv6 SLA nebo ekvivalentní technologie	ANO	ANO
uRPF pro IPv6	ANO	ANO
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	ANO	ANO
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie	ANO	ANO
DHCPv6 Relay	ANO	ANO
Statefull NAT64	ANO	ANO
Min. počet NAT64 spojení (statefull)	8M	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
QoS Shaping and Policing	ANO	ANO
Class Based and Priority queuing	ANO	ANO
Rate Limiting	ANO	ANO
Hierarchical QoS	min. 3 úrovně	ANO
RSVP	ANO	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	50	ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO	ANO
ACL na rozhraní IN/OUT	ANO	ANO
IPSec AES-GCM-256	ANO	ANO
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	ANO	ANO
QoS pre-classification pro IPSec	ANO	ANO
Minimální šifrovací výkon pro IPSec AES 256 (IMIX provoz)	5Gb/s	ANO
IPSec IKEv2	ANO	ANO
VRF aware IPSec	ANO	ANO
SHA-2 (SHA-256, SHA-512)	ANO	ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	ANO	ANO
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	ANO	ANO
Podpora Suite-B šifrovacích algoritmů (RFC 6379) ve spojení s GDOI based VPN	ANO	ANO
VRF aware GDOI group member (selektivní šifrování provozu per IP VPN)	ANO	ANO

Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS, bez nutnosti dešifrování paketů	ANO	ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - využívané pásmo	ANO	ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - odezvy aplikací	ANO	ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, reálných a aplikačních toků - počty aplikačních spojení	ANO	ANO
Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky	ANO	ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	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 type	ANO	ANO
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	ANO	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	ANO
Model-driven telemetry pro real-time streaming informací o stavu zařízení	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloADERu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchors	ANO	ANO
Podpora Secure Unique Device Identity (IEEE 802.1AR) pro ověření autentičnosti HW prostředků zařízení	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Python scripting	ANO	ANO
Software patching	ANO	ANO
SNMPv2/v3	ANO	ANO

TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

Komponenta	Požadavek na funkcionalitu	Minimální požadavky	Název (typ) modulu	Splňuje ANO/NE
	Základní vlastnosti			
Modul_AM1	Rozšíření o 1GE s volitelným fyzickým rozhraním	min. 2x 1GE	FLSA1-HX-2X1GE=	ANO
Modul_AM2	Rozšíření o 10GE s volitelným fyzickým rozhraním	min. 2x 10GE	FLSA1-HX-2X10GE=	ANO
Modul_AM3	Rozšíření 1GE portu o IEEE 802.1ae	ANO	FLSA1-MACSEC1G=	ANO
Modul_AM4	Rozšíření 10GE portu o IEEE 802.1ae	ANO	FLSA1-MACSEC10G=	ANO
Modul_AM5	Rozšíření o 40GE s volitelným fyzickým rozhraním	min. 1x 40GE	EPA-1X40GE=	ANO
Modul_AM6	Rozšíření o 40GE s volitelným fyzickým rozhraním	min. 2x 40GE	EPA-2X40GE=	ANO
Modul_AM7	Rozšíření krypto propustnosti na	min. 15 Gbit/s	FLSA1-2HX8G16G=	ANO
Modul_AM8	Rozšíření krypto propustnosti na	min. 25 Gbit/s	FLSA1-2HX8G25G=	ANO

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	koncové zařízení videokonferencí	CS-BOARD55S-G-K9
Dedikovaný videokonferenční HW pro skupinové použití	Ano	Ano
Plně integrované zařízení (kodek, kamera, monitor, stojan, mikrofon a ozvučení tvoří jeden kompaktní celek)	Ano	Ano
Velikost, rozlišení a poměr obrazovky	55" LED display (4k, 16:9)	Ano
Specifikace displeje	Počet barev: 1,07 miliardy (10 bitů), Kontrast: 1: 4000, Doba odezvy: 5,5 ms	Ano
Kapacitní dotykový displej	Ano	Ano
Multi-touch	Ano	Ano
Ochranné sklo s optickou vazbou	Ano	Ano
Touch pen pro kreslení a psaní na multi-touch displej a pro whiteboarding	Ano	Ano
Zorný uhel	89 stupňů (všechny směry)	Ano
12x vestavěný mikrofon s inteligentním hlasovým sledováním	Ano	Ano
Integrované reproduktory optimalizované pro hlas	Ano	Ano
Kamera v rozlišení 4K	Ano	Ano
Pevná čočka, nekonečné zaostření	Ano	Ano
Horizontální zorné pole	83°	Ano
Vertikální zorné pole	55°	Ano
Náklon kamery	-25°	Ano
Vstupy a výstupy	1x HDMI, 1x 3.5 mini jack, 2x USB 3.0	Ano
Video vstupy	1x HDMI pro prezentaci nebo sdílení, Místní prezentace až do 4K, Audio přes HDMI, Rychlost snímku 60 fps pro 1080p a 30 fps pro 2160p	Ano
Rozlišení živého vstupu a sdílené prezentace	HD 1080p30	Ano

Musí být možné na tomto zařízení bezdrátově zobrazit a sdílet plochu Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele	Ano	Ano
Musí být možné na tomto zařízení bezdrátově zobrazit, nasdílet a v reálném čase editovat whiteboard (kreslicí plochu) s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele pro Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší, iOS 9.0 a vyšší, Android 4.1 a vyšší	Ano	Ano
Síťové rozhraní	1x Eth (RJ-45) 100/1000 Mbps, Wi-Fi 802.11a/b/g/n/ac (2.4 a 5 Ghz)	Ano
Zařízení podporuje dynamické, nebo statické přidělování adres pro IPv4	Ano	Ano
Zařízení je Bluetooth ready	Ano	Ano
Uživatelské rozhraní přímo z dotykového displeje, nebo pomocí aplikace na osobním mobilním zařízení	Ano	Ano
Správa systému pomocí Cloud-ové služby ve které se zařízení registruje	Ano	Ano
Zařízení pro komunikaci s Cloud-ovými službami využívá RESTful APIs	Ano	Ano
Veškerá další komunikace – s jinými zařízeními, mobilními aplikacemi a řešeními třetích stran probíhá v Cloudu	Ano	Ano
Podpora českého a anglického jazyka	Ano	Ano
Real-time media jsou šifrované pomocí SRTP protokolu	Ano	Ano
End-to-End komunikace využívá zabezpečení AES (128), AES 256, SHA1, SHA256 a RSA	Ano	Ano
Nároky na datovou propustnost	od 768 Kbps pro 720p30 od 1.72 Mbps pro 1080p30	Ano
Video formáty CIF, w288p, 448p, w448p, 4CIF, w576p, VGA, SVGA, XGA, WXGA, 720p, 1080p	ano, příjem i vysílání	Ano
Schválení a soulad - Směrnice (2014/35/EU, 2014/30/EU, 2014/53/EU, 2011/65/EU, 2002/96/EC), Schváleno NRTL (bezpečnost výrobků), FCC CFR 47 Part 15B (EMC) – Class A, FCC (rádiové zařízení)	Ano	Ano
Akustické potlačení ozvěny	Ano	Ano
Automatic gain control (AGC)	Ano	Ano
Automatic noise reduction	Ano	Ano
Active lip synchronization	Ano	Ano

Lokální a serverové adresáře	Ano	Ano
Registr volaných, přijatých a zmeškaných spojení	Ano	Ano
Připojení zařízení k centralizovanému řízení, min. 3-letý provoz	Ano	Ano

Prvek_AO

Požadavek na funkcionalitu	Minimální požadavk	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	koncové zařízení	CS-BOARD85S-G-K9
Dedikovaný videokonferenční HW pro skupinové použití	Ano	Ano
Plně integrované zařízení (kodek, kamera, monitor, stojan, mikrofon a ozvučení tvoří jeden kompaktní celek)	Ano	Ano
Velikost, rozlišení a poměr obrazovky	85" LED display (4k, 16:9)	Ano
Specifikace displeje	Počet barev: 1,07 miliardy (10 bitů), Kontrast: 1: 4000, Doba odezvy: 6,5 ms	Ano
Kapacitní dotykový displej	Ano	Ano
Multi-touch	Ano	Ano
Ochranné sklo s optickou vazbou	Ano	Ano
Touch pen pro kreslení a psaní na multi-touch displej a pro whiteboarding	Ano	Ano
Zorný uhel	89 stupňů (všechny směry)	Ano
12x vestavěný mikrofon s inteligentním hlasovým sledováním	Ano	Ano
Integrované reproduktory optimalizované pro hlas	Ano	Ano
Kamera v rozlišení 4K	Ano	Ano
Pevná čočka, nekonečné zaostření	Ano	Ano
Horizontální zorné pole	83°	Ano
Vertikální zorné pole	55°	Ano
Náklon kamery	-25°	Ano
Vstupy a výstupy	1x HDMI, 1x 3.5 mini jack, 1x USB C, 1x USB micro	Ano

Video vstupy	1x HDMI pro prezentaci nebo sdílení, Místní prezentace až do 4K, Audio přes HDMI, Rychlost snímku 60 fps pro 1080p a 30 fps pro 2160p	Ano
Rozlišení živého vstupu a sdílené prezentace	HD 1080p30	Ano
Musí být možné na tomto zařízení bezdrátově zobrazit a sdílet plochu Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele	Ano	Ano
Musí být možné na tomto zařízení bezdrátově zobrazit, nasdílet a v reálném čase editovat whiteboard (kreslicí plochu) s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele pro Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší, iOS 9.0 a vyšší, Android 4.1 a vyšší	Ano	Ano
Síťové rozhraní	1x Eth (RJ-45) 100/1000 Mbps, Wi-Fi 802.11a/b/g/n/ac (2.4 a 5 Ghz)	Ano
Zařízení podporuje dynamické, nebo statické přidělování adres pro IPv4 / IPv6	Ano	Ano
Zařízení je Bluetooth ready	Ano	Ano
Podpora NTP, HTTP/HTTPS, TLS proxy, CDP, 802.1x, 802.1Q, 802.1p	Ano	Ano
Uživatelské rozhraní přímo z dotykového displeje, nebo pomocí aplikace na osobním mobilním zařízení	Ano	Ano
Správa systému pomocí Cloud-ové služby ve které se zařízení registruje	Ano	Ano
Zařízení pro komunikaci s Cloud-ovými službami využívá RESTful APIs	Ano	Ano
Veškerá další komunikace – s jinými zařízeními, mobilními aplikacemi a řešeními třetích stran probíhá v Cloudu	Ano	Ano

Podpora českého a anglického jazyka	Ano	Ano
Real-time media jsou šifrované pomocí SRTP protokolu	Ano	Ano
End-to-End komunikace využívá zabezpečení AES (128), AES 256, SHA1, SHA256 a RSA	Ano	Ano
Nároky na datovou propustnost	od 768 Kbps pro 720p30 od 1.72 Mbps pro 1080p30	Ano
Video formáty CIF, w288p, 448p, w448p, 4CIF, w576p, VGA, SVGA, XGA, WXGA, 720p, 1080p	ano, příjem i vysílání	Ano
Schválení a soulad - Směrnice (2014/35/EU, 2014/30/EU, 2014/53/EU, 2011/65/EU, 2002/96/EC), Schváleno NRTL (bezpečnost výrobků), FCC CFR 47 Part 15B (EMC) – Class A, FCC (rádiové zařízení)	Ano	Ano
Akustické potlačení ozvěny	Ano	Ano
Automatic gain control (AGC)	Ano	Ano
Automatic noise reduction	Ano	Ano
Active lip synchronization	Ano	Ano
Lokální a serverové adresáře	Ano	Ano
Registr volaných, přijatých a zmeškaných spojení	Ano	Ano
Připojení zařízení k centralizovanému řízení, min. 3-letý provoz	Ano	Ano

Požadavek na funkcionalitu	Minimální požadaví	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	koncové zařízení videokonferencí	CS-KIT-K9
Dedikovaný videokonferenční HW pro skupinové použití	Kodek, kamera, mikrofon a ozvučení tvoří jeden kompaktní celek	Ano
6x vestavěný mikrofon s inteligentním hlasovým sledováním	Ano	Ano
Integrované reproduktory optimalizované pro hlas	Pět reproduktorů ve vyvážené konfiguraci	Ano
Kamera v rozlišení 5K UltraHD	Ano	Ano
Pevná čočka. Vzdálenost zaostření 1 m až nekonečno	Ano	Ano
3x Zoom	Ano	Ano
Horizontální zorné pole	83°	Ano
Vertikální zorné pole	51.5°	Ano
Automatické zaostření, jas a vyvážení bílé	Ano	Ano
Auto framing pro detekci zvuku a tváře	Ano	Ano
Zvukové standardy G.711, G.722, G.722.1, G.729, AAC-LD, a Opus	Ano	Ano
Musí být možné na tomto zařízení bezdrátově zobrazit a sdílet plochu Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele	Ano	Ano
Zařízení podporuje dynamické, nebo statické přidělování adres pro IPv4 a IPv6	Ano	Ano
Zařízení podporuje Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ, 802.1x, 802.1Q, 802.1p, URI dialing	Ano	Ano
Uživatelské rozhraní přímo z kontrolního panelu, nebo pomocí aplikace na osobním mobilním zařízení	Ano	Ano
Správa systému pomocí Cloud-ové nebo On-prem služby ve které se zařízení registruje	Ano	Ano
Zařízení pro komunikaci s Cloud-ovými službami využívá RESTful APIs	Ano	Ano
End-to-End komunikace využívá zabezpečení AES, H.235 v3, H.323 a SIP point-to-point	Ano	Ano

Nároky na datovou propustnost	od 768 Kbps pro 720p30 od 1.152 Mbps pro 720p60 od 1.472 Mbps pro 1080p30 od 2.56 Mbps pro 1080p60	Ano
Rozlišení živého vstupu a sdílené prezentace	HD 1080p60/p30	Ano
Schválení a soulad - Směrnice (2014/35/EU, 2014/30/EU, 2014/53/EU, 2011/65/EU, 2002/96/EC), Schváleno NRTL (bezpečnost výrobků), FCC CFR 47 Part 15B (EMC) – Class A, FCC (rádiové zařízení)	Ano	Ano
Automatic gain control (AGC)	Ano	Ano
Automatická redukce šumu	Ano	Ano
Aktivní synchronizace rtů	Ano	Ano
Lokální a serverové adresáře	Ano	Ano
Registr volaných, přijatých a zmeškaných spojení	Ano	Ano
Vstupy a výstupy	1x HDMI, 1x 3.5 mini jack, 1x USB 2.0, 1x USB micro	Ano
Video vstupy	1x HDMI s podporou formátu 4Kp30, HD1080p60	Ano
Video výstupy	2x HDMI s podporou formátu 4kp60	Ano
Zvukové vstupy	2x mikrofón, 4-pin mini-jack, 1x Audio in přes HDMI, Integrovaný mikrofón	Ano
Zvukové výstupy	1x Line out mini-jack (stereo)	Ano
Zařízení je Bluetooth 4.0 LE	Ano	Ano

Síťové rozhraní	1x Eth (RJ-45) 100/1000 Mbps, 1x Eth (RJ-45) pro kontrolní panel Wi-Fi 802.11a/b/g/n/ac (2.4 a 5 Ghz)	Ano
Připojení zařízení k centralizovanému řízení, min. 3-letý provoz	Ano	Ano

Prvek_AQ

Požadavek na funkcionalitu	Minimální požadaví	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	koncové zařízení videokonferencí	CS-KIT-MINI-K9
Typ zařízení - Dedikovaný videokonferenční HW pro skupinové použití	Kodek, kamera, mikrofon a ozvučení tvoří jeden kompaktní celek	Ano
Vestavěný mikrofon s inteligentním hlasovým sledováním	Ano	Ano
Integrované reproduktory optimalizované pro hlas	Tři reproduktory ve vyvážené konfiguraci	Ano
Kamera v rozlišení 4K UltraHD	Ano	Ano
Pevná čočka. Vzdálenost zaostření 1 m až nekonečno	Ano	Ano
2x Zoom	Ano	Ano
Horizontální zorné pole	120°	Ano
Automatické zaostření, jas a vyvážení bílé	Ano	Ano
Auto framing pro detekci zvuku a tváře	Ano	Ano
Zvukové standardy G.711, G.722, G.722.1, G.729, AAC-LD, a Opus	Ano	Ano
Musí být možné na tomto zařízení bezdrátově zobrazit a sdílet plochu Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele	Ano	Ano
Zařízení podporuje dynamické, nebo statické přidělování adres pro IPv4 a IPv6	Ano	Ano
Zařízení podporuje Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ, 802.1x, 802.1Q, 802.1p, URI dialing	Ano	Ano
Uživatelské rozhraní přímo z kontrolního panelu, nebo pomocí aplikace na osobním mobilním zařízení	Ano	Ano
Správa systému pomocí Cloud-ové nebo On-prem služby ve které se zařízení registruje	Ano	Ano
Zařízení pro komunikaci s Cloud-ovými službami využívá RESTful APIs	Ano	Ano
End-to-End komunikace využívá zabezpečení AES, H.235 v3, H.323 a SIP point-to-point	Ano	Ano

Nároky na datovou propustnost	od 768 Kbps pro 720p30 od 1.152 Mbps pro 720p60 od 1.472 Mbps pro 1080p30 od 2.56 Mbps pro 1080p60	Ano
Rozlišení živého vstupu a sdílené prezentace	HD 1080p60/p30	Ano
Schválení a soulad - Směrnice (2014/35/EU, 2014/30/EU, 2014/53/EU, 2011/65/EU, 2002/96/EC), Schváleno NRTL (bezpečnost výrobků), FCC CFR 47 Part 15B (EMC) – Class A, FCC (rádiové zařízení)	Ano	Ano
Automatic gain control (AGC)	Ano	Ano
Automatická redukce šumu	Ano	Ano
Aktivní synchronizace rtů	Ano	Ano
Lokální a serverové adresáře	Ano	Ano
Registr volaných, přijatých a zmeškaných spojení	Ano	Ano
Vstupy a výstupy	1x HDMI, 1x 3.5 mini jack, 2x USB 2.0, 1x USB micro	Ano
Video vstupy	1x HDMI s podporou formátu 4Kp30, HD1080p60	Ano
Video výstupy	1x HDMI s podporou formátu 4kp60	Ano
Zvukové vstupy	1x Audio in přes HDMI, Integrovaný mikrofón	Ano
Zvukové výstupy	1x Line out mini-jack (stereo)	Ano
Zařízení je Bluetooth 4.0 LE	Ano	Ano

Síťové rozhraní	1x Eth (RJ-45) 100/1000 Mbps, 1x Eth (RJ-45) pro kontrolní panel Wi-Fi 802.11a/b/g/n/ac (2.4 a 5 Ghz)	Ano
Schopnost poskytovat video, mikrofon a reproduktory přes jeden kabel USB do připojeného počítače	Ano, podpora USB pass-through	Ano
Připojení zařízení k centralizovanému řízení, min. 3-letý provoz	Ano	Ano

Požadavek na funkcionalitu	Minimální požadaví	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	koncové zařízení videokonferencí	CS-ROOM55-K9
Dedikovaný videokonferenční HW pro skupinové použití	Ano	Ano
Plně integrované zařízení (kodek, kamera, monitor, stojan, mikrofon a ozvučení tvoří jeden kompaktní celek)	Ano	Ano
Velikost, rozlišení a poměr obrazovky	55" LED display (4k, 16:9)	Ano
Specifikace displeje	Počet barev: 1,07 miliardy (10 bitů), Kontrastní poměr: Typický 1100, Úhel pohledu: +/- 178 stupňů, Doba odezvy: 8 ms	Ano
6x vestavěný mikrofon s inteligentním hlasovým sledováním	Ano	Ano
Integrovaný reproduktorový systém s levým, středním a pravým kanálem plus basový reproduktor	Pět reproduktorů ve vyvážené konfiguraci	Ano
Kamera v rozlišení 5K UltraHD	Ano	Ano
Pevná čočka. Vzdálenost zaostření 1 m až nekonečno	Ano	Ano
3x Zoom	Ano	Ano
Horizontální zorné pole	83°	Ano
Vertikální zorné pole	51.5°	Ano
Automatické zaostření, jas a vyvážení bílé	Ano	Ano
Auto framing pro detekci zvuku a tváře	Ano	Ano
Zvukové standardy G.711, G.722, G.722.1, G.729, AAC-LD, a Opus	Ano	Ano
Musí být možné na tomto zařízení bezdrátově zobrazit a sdílet plochu Windows 7 a vyšší, Mac OS X Mavericks 10.10 a vyšší s použitím bezplatně stažitelné aplikace a připojením k internetu (do cloudu výrobce zařízení) a to i bez nutnosti připojení k bezdrátové síti Zadavatele	Ano	Ano
Zařízení podporuje dynamické, nebo statické přidělování adres pro IPv4 a IPv6	Ano	Ano
Zařízení podporuje Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ, 802.1x, 802.1Q, 802.1p, URI dialing	Ano	Ano
Uživatelské rozhraní přímo z kontrolního panelu, nebo pomocí aplikace na osobním mobilním zařízení	Ano	Ano
Správa systému pomocí Cloud-ové nebo On-prem služby ve které se zařízení registruje	Ano	Ano

Zařízení pro komunikaci s Cloud-ovými službami využívá RESTful APIs	Ano	Ano
End-to-End komunikace využívá zabezpečení AES, H.235 v3, H.323 a SIP point-to-point	Ano	Ano
Nároky na datovou propustnost	od 768 Kbps pro 720p30 od 1.152 Mbps pro 720p60 od 1.472 Mbps pro 1080p30 od 2.56 Mbps pro 1080p60	Ano
Rozlišení živého vstupu a sdílené prezentace	HD 1080p60/p30	Ano
Schválení a soulad - Směrnice (2014/35/EU, 2014/30/EU, 2014/53/EU, 2011/65/EU, 2002/96/EC), Schváleno NRTL (bezpečnost výrobků), FCC CFR 47 Part 15B (EMC) – Class A, FCC (rádiové zařízení)	Ano	Ano
Automatic gain control (AGC)	Ano	Ano
Automatická redukce šumu	Ano	Ano
Aktivní synchronizace rtů	Ano	Ano
Lokální a serverové adresáře	Ano	Ano
Registr volaných, přijatých a zmeškaných spojení	Ano	Ano
Vstupy a výstupy	1x USB 2.0, 1x USB micro	Ano
Video vstupy	2x HDMI s podporou formátu 4Kp30, HD1080p60 (HDMI 2 podporuje obsah HDCP pro místní prohlížení)	Ano
Video výstupy	1x HDMI s podporou formátu 4kp60	Ano
Zvukové vstupy	2x mikrofón, 4-pin mini-jack, 2x Audio in přes HDMI, Integrovaný mikrofón	Ano
Zvukové výstupy	1x Line out mini-jack (stereo)	Ano
Zařízení je Bluetooth 4.0 LE	Ano	Ano

Síťové rozhraní	1x Eth (RJ-45) 100/1000 Mbps, 1x Eth (RJ-45) pro kontrolní panel Wi-Fi 802.11a/b/g/n/ac (2.4 a 5 Ghz)	Ano
Připojení zařízení k centralizovanému řízení, min. 3-letý provoz	Ano	Ano

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	videokonferenční bridge	CTI-CMS1KM5-BUN-K9
Uživatelské, funkční požadavky		
Podpora audio a video konferenčních seminářů.	ANO	ANO
Sdílení desktopového prostředí s možností výběru jednoho specifického dokumentu nebo aplikace.	ANO	ANO
Připojení do konferenčního semináře	ANO	ANO
Nativní aplikací (tlustý klient) – MS Win7/10, Mac OS, iOS, Android	ANO	ANO
Webový prohlížeč (bez nutnosti instalace dodatečných plug-in modulů - WebRTC)	ANO	ANO
Volání z videokonferenční jednotky (SIP/H323/volání na IP adresu)	ANO	ANO
Připojení účastníka z platformy Skype For Bussines	ANO	ANO
Možnost plánování semináře v prostředí kalendářových služeb	ANO	ANO
Odpovídající klientské aplikace pro kalendářové plánování v desktopovém prostředí i v mobilních klientech.	ANO	ANO
Plánovací nástroje ve webovém prostředí platformy.	ANO	ANO
Organizace účastníků semináře	ANO	ANO
Zobrazení seznamu	ANO	ANO
Ztlumení všech účastníků	ANO	ANO
Ztlumení vybraného účastníka	ANO	ANO
Manuální přizvání účastníka (dial-out, přeposlání pozvánky)	ANO	ANO
Manuální vyřazení účastníka ze semináře.	ANO	ANO
Ověření účastníků jméno/heslo	ANO	ANO
Anonymní účastník	ANO	ANO
Uzamknutí semináře, PIN	ANO	ANO
Rozdělení rolí účastníků semináře	ANO	ANO
Hostitel, zřizovatel semináře	ANO	ANO
Prezentující	ANO	ANO
Běžný účastník	ANO	ANO
Rízení rozložení obrazu	ANO	ANO
Prezentující	ANO	ANO
Prezentující + prezentovaný obsah	ANO	ANO
Prezentovaný obsah	ANO	ANO
Pořízení záznamu semináře	ANO	ANO
Záznam prezentovaného obsahu	ANO	ANO
Nároky na provoz a správu systému		
Provoz a užívání formou serverové platformy, instalované aplikace.	ANO	ANO
Forma licencování	ANO	ANO
Na souběžně běžící seminář.	ANO	ANO
Kapacita semináře není licenčně omezena.	ANO	ANO
Technické parametry	ANO	ANO
Podpora IPv4	ANO	ANO
Podpora IPv6	ANO	ANO
Video kodeky H263, H264 SVC/AVC	ANO	ANO

Video kodeky HTML5/WebRTC, VP8, MS RTV	ANO	ANO
Video rozlišení až do FullHD 1080/60	ANO	ANO
Rozlišení prezentačního kanálu až do FullHD 1080/30	ANO	ANO
Audio kodeky G711a/u, G722	ANO	ANO
Audio kodeky AAC-LD, Opus	ANO	ANO
Pořízení záznamu až do FullHD 1080/30	ANO	ANO
Streamování záznamu až do HD 720/30	ANO	ANO
Zabezpečení použité platformy.	ANO	ANO
Media Audio/Video – AES/SRTP	ANO	ANO
Signalizace SSL/TLS	ANO	ANO
Použití certifikátů, podpora certifikační autority	ANO	ANO
DNSSEC	ANO	ANO
Správa a provoz	ANO	ANO
Přístup na admin portál - https	ANO	ANO
Syslog	ANO	ANO
NTP	ANO	ANO
CDR záznamy	ANO	ANO
Zálohování a obnova systému	ANO	ANO
Podpora virtualizace platformy	ANO	ANO
Podpora vysoké dostupnosti, provoz ve více datových centrech.	ANO	ANO
Skalování formou clusteru, rozšířením dalšího serverového uzlu.	ANO	ANO
Rozkládání zátěže, kaskádování semináře přes více uzlů.	ANO	ANO
Správa uživatelů	ANO	ANO
Microsoft AD	ANO	ANO
LDAP	ANO	ANO
Lokálně definovaný uživatel	ANO	ANO
Administrátorské prostředí	ANO	ANO
Možnost definování více administrátorů	ANO	ANO
Požadovaná kapacita platformy pro 3-letý provoz	ANO	ANO
Počet souběžně běžících seminářů 10.	ANO	ANO
Počet souběžně nahrávaných seminářů 10.	ANO	ANO
Počet účastníků semináře minimálně 100.	ANO	ANO
Celkový počet účastníků souběžně běžících seminářů minimálně 200.	ANO	ANO
Účastníkem schůzky kdokoliv kdo má „pozvánku“ a splňuje požadavky na připojení. Instalace „tlustého“ klienta není zpoplatněna.	ANO	ANO
Programovatelnost, API		
Podporované REST API služby	ANO	ANO
Vytváření virtuálního semináře, přiřazení účastníků	ANO	ANO
Manipulace s aktivním videokonferenčním hovorem, technické parametry.	ANO	ANO
Organizace účastníků, seznamy, manipulace s jednotlivci	ANO	ANO
Práce s účastníky, uživateli.	ANO	ANO
Nastavování systémových parametrů, diagnostika.	ANO	ANO
Záznamy seminářů, aktivace.	ANO	ANO
Streamování semináře, aktivace.	ANO	ANO

Příloha č. 2 Specifikace školení

Název školení	Obsah
ICND1 – Interconnecting Cisco Networking Devices Part 1	<p>Základní funkce IP datových sítí, OSI a TCP/IP model, síťová média a typy kabeláže</p> <p>Technologie LAN přepínačů - základní konfigurace přepínače, VLAN sítě, konfigurace Trunk rozhraní</p> <p>IP adresace (IPv4/IPv6)</p> <p>Technologie IP směrování v IP sítích</p> <p>Statické a dynamické směrování (OSPF), směrování mezi různými VLAN</p> <p>Nastavení DHCP, ACL, NAT, Overloading</p> <p>Nastavení zabezpečení síťových zařízení - SSH, nastavení hesel, Port security</p> <p>Řešení problémů v datových sítích</p>
ICND2 – Interconnecting Cisco Networking Devices Part 2	<p>Implementace středně velké přepínané sítě - řešení problémů s VLAN, optimalizace STP</p> <p>Řešení problémů základní konektivity - IPv4 a IPv6</p> <p>Konfigurace, verifikace a řešení problému EIGRP - IPv4 a IPv6</p> <p>Konfigurace, verifikace a řešení problému multi-area OSPF - IPv4 a IPv6 (OSPFv3)</p> <p>Wide Area Networks - Konfigurace PPP, CHAP a PAP, Frame Relay, VPN a GRE tunely</p> <p>Správa Cisco zařízení - záloha konfigurací a software, licence, SNMP, syslog a NetFlow</p>
EXAM 200 - 125 CCNA Cisco Certified Network Associate (803)	<p>CCNA Composite Exam: The 200-120 CCNAX is the composite exam associated with the Cisco CCNA Routing and Switching certification. Candidates can prepare for this exam by taking the Interconnecting Cisco Networking Devices: Accelerated (CCNAX) course. This exam tests a candidate's knowledge and skills required to install, operate, and troubleshoot a small to medium size enterprise branch network. The topics include all the areas covered under ICND 1 and ICND2 Exams.</p>
ROUTE – IMPLEMENTING CISCO IP ROUTING	<p>Směrovací protokoly</p> <p>Plánování rozsáhlých směrovaných sítí</p> <p>Konfigurace směrování</p> <p>Ověření konfigurace</p> <p>Jednotlivá dostupná zařízení</p>
EXAM 300-101 IMPLEMENTING CISCO IP ROUTING	<p>Implementing Cisco IP Routing (ROUTE 300-101) is a qualifying exam for the Cisco CCNP Routing and Switching and CCDP certifications. The ROUTE 300-101 exam certifies the routing knowledge and skills of successful candidates. They are certified in using advanced IP addressing and routing in implementing scalable and highly secure Cisco routers that are connected to LANs, WANs, and IPv6.</p>

<p>SWITCH – IMPLEMENTING CISCO IP SWITCHED NETWORKS</p>	<p>Design přepínaných sítí, Cisco Enterprise Composite Network model VLAN, privátní VLAN, trunking (ISL, IEEE 802.1q), VTP, DHCP IPv4/IPv6, Etherchannel Spanning tree protokoly STP, RSTP, PVSTP+, RPVSTP+ a MSTP Směrování mezi VLAN HW, SW redundance v přepínaných sítích - FHRP IPv4/IPv6 - HSRP, VRRP, GLBP Virtualizace přepínačů - StackWise, VSS Monitoring sítě - SNMP, IP SLA Bezpečnostní funkce v přepínané infrastruktuře</p>
<p>EXAM 300-115 - IMPLEMENTING CISCO IP SWITCHED NETWORKS</p>	<p>Implementing Cisco IP Switched Networks (SWITCH 300-115) is a qualifying exam for the Cisco CCNP Routing and Switching and CCDP certifications. The SWITCH 300-115 exam certifies the switching knowledge and skills of successful candidates. They are certified in planning, configuring, and verifying the implementation of complex enterprise switching solutions that use the Cisco Enterprise Campus Architecture.</p>
<p>DESIGN – DESIGNING FOR CISCO INTERNETWORK SOLUTIONS</p>	<p>Metodologie návrhu sítí Strukturalizace a modularizace návrhu sítí Návrh sítí v campusu a v datových centrech Design vzdáleného připojení IP adresace a routovací protokoly Security řešení pro sítě Identifikace síťových požadavků pro voice Identifikace síťových požadavků pro wireless Implementace a zprovoznění síťového designu</p>
<p>EXAM 640 - 864 DESIGNING FOR CISCO INTERNETWORK SOLUTIONS</p>	<p>This exam requires a foundation or apprentice knowledge of network design for the Cisco converged networks based on borderless network architecture. CCDA certified professionals can design routed and switched network infrastructures and services involving LAN, WAN, wireless, and broadband access for businesses and organizations.</p>
<p>TSHOOT – TROUBLESHOOTING AND MAINT. CISCO IP NETWORKS</p>	<p>Rozbor metod a přístupů řešení problémů v komplexních datových sítích Aplikace vhodných metod a nástrojů pro efektivní řešení specifických problémů Řešení problémů v přepojovaných lokálních sítích (problematika VLAN, VACL, port security, STP, Inter-VLAN Routing, FHRP) Řešení problémů ve směrovaných sítích (problematika směrovacích protokolů EIGRP, OSPF a BGP, L3 path control) včetně IPv6 sítí. Problematika bezpečnostních funkcí a jejich vliv na způsob řešení problémů (Port-security a AAA) Řešení problémů v komplexním prostředí</p>

<p>EXAM 300-135 TROUBLESHOOTING AND MAINTAINING CISCO IP NETWORKS</p>	<p>Troubleshooting and Maintaining Cisco IP Networks (TSHOOT 300-135) is a qualifying exam for the Cisco CCNP Routing and Switching certification. The TSHOOT 300-135 exam certifies that the successful candidate has the knowledge and skills necessary to:</p> <p>Plan and perform regular maintenance on complex enterprise routed and switched networks Use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting</p>
<p>ARCH – DESIGNING CISCO NETWORK SERVICES ARCHITECTURE</p>	<p>Podrobná metodika návrhu logické oblasti Enterprise Campus (moduly Campus Infrastructure, Network Management, Server Farm, Edge Distribution) a logické oblasti Enterprise Edge (moduly WAN, Remote Access & VPN, Internet Connectivity, E-Commerce)</p> <p>Návrh síťové správy a managementu Návrh služeb vysoké dostupnosti (high availability) Návrh efektivní IP adresace (segmentace) Návrh škálovatelného a efektivního směrování Návrh datacentrových řešení v Enterprise Campus Návrh bezpečnostního řešení Návrh hardwarové virtualizace (VSS, vPC, StackWise) Návrh QoS Návrh Multicast služeb Návrh VPN sítí Návrh bezdrátových sítí Návrh řešení IP telefonie</p>
<p>EXAM 642 - 874 DESIGNING CISCO NETWORK SERVICE ARCHITECTURES</p>	<p>The 642-874 and technologies, including network infrastructure, intelligent network services and converged network solutions. Candidates can prepare for this exam by taking the ARCH Designing Cisco Network Service Architectures course.</p>
<p>DCNX1K – Implementing the Cisco Nexus 1000V</p>	<p>obecný popis platformy VMware vSphere (rychlé zopakování základních pojmů) virtuální přepínač a distribuovaný virtuální přepínač popis produktu Cisco Nexus 1000V, jeho architektury, vyjasnění základních pojmů instalace přepínače Cisco Nexus 1000V základní konfigurace pokročilé vlastnosti (zabezpečení, kvalita služby, řízení přístupu) řešení možných problémů s přepínačem Nexus 1000V</p>
<p>DCNX5K – Configuring Cisco Nexus 5000 Switches</p>	<p>Přehled produktového portfolia přepínačů Nexus Architektura přepínačů Nexus 5000 a 2000 Fyzická instalace Konfigurace základních a pokročilých L2 funkcí Konfigurace správy a dohledu Rychlý přehled protokolu FC (fibre channel) Popis protokolu FCoE (fibre channel over ethernet) a jeho konfigurace Analýza a řešení možných problémů</p>

DCID školení	<p>Popis forwardingu L2 a L3 v DC, kabeláž, rack design, access, aggregate a core vrstva Design vPC, FabricPath, OTV, and LISP v prostředích zákazníka a popis možnosti managementu v LAN. Popis hardware virtualizace a FEX technologie, srovnání Nexus 1000v s VM-FEX, bezpečnostní hrozby uvnitř DC a Virtual Application Container Services pro IaaS, popis managementu a možností automatizace DC infrastruktury. Popis možností storage a RAID, popis konceptů Fibre Channel , design Fibre Channel a FCoE sítí, možnosti managementu. Popis UCS C-Series, M-Series, a B-Series serverů, možnosti konektivity a adaptéry. Popis UCS -B blade schassis, I/O moduly, a fabric interconnect. Srovnání EHV a NPV modů. Návrh resource parametrů pro UCS, základní nastavení, IP adresace, RBAC, nastavení autentikace apod. Nastavení resource poolů a politik použitých v UCS service profilech a templatech.</p>
DCII školení	<p>Konfigurace RSTP, MST, port channel a implementace Cisco FabricPath, OTV, VXLAN, a LISP Konfigurace first-hop redundancy, routingu, a multicastu v datovém centru Konfigurace user management a system security funkcí na Nexus switchích Základní konfigurace Fibre Channel, Fibre Channel domeny, a Fibre Channel port security Konfigurace FCoE Konfigurace distributed device aliases, zoning, NPV, a FCIP Konfigurace system managementu a monitoring infrastruktury</p>
DCUCI školení	<p>Obecný úvod UCS. Detailní popis UCS architektury a jednotlivých funkčních částí. Instalace UCS hardware. Popis konsolidované I/O fabriky. Upgrade systému UCS. Seznámení s CS Managerem. Konfigurace systému za pomoci UCS Manageru. Popis připojení do sítě LAN. Popis připojení do sítě SAN. Řízení zdrojů a virtualizace parametrů hardware. Záloha a obnovení systému. Návrh a konfigurace vysoké dostupnosti a monitoring systému. Představení switche Nexus 1000V. Instalace a konfigurace Nexus 1000V.</p>

DCVAI školení	<p>Funkce přepínačů Nexus Virtuální kontexty přepínačů (VDC) LAN Overlay sítě (VXLAN) Základy virtualizačních technologií Technologie Fabric Extender (FEX) FabricPath Koncept Unified Fabric (DCB, FCoE) Unified Computing System (UCS) Správa UCS Manager Automatizace a orchestrace v datovém centru Základy Cloud Computing Přehled vlastností UCS Director Application-Centric Infrastructure (ACI) Programování a orchestrace ACI Praktické laby</p>
DCIT školení	<p>Troubleshooting L2 technologií, jako STP, port channel, vPC, FabricPath, a FEX Troubleshooting first-hop redundance, routing, a CFS uvnitř data centra Troubleshooting virtualizačních řešení, jako jsou OTV, VRF, a VXLAN Troubleshooting storage area networks (SAN), Fibre Channel, FCoE, zoning, NPV a NPIV Troubleshooting data center unified computing</p>
IINS – Implementing Cisco IOS Network Security	<p>Základy síťové bezpečnosti Bezpečnostní politiky, životní cyklus Cisco "Borderless Networks" koncept Cisco Network Foundation Protection Administrace a konfigurace směrovačů pomocí CCP Základní kroky pro zabezpečení směrovače Konfigurace AAA modelu pomocí Cisco ACS, Lokální databáze Zabezpečení Cisco přepínačů, L2 bezpečnost IPv6 základní vlastnosti, Filtrace pomocí IPv6 ACL Eliminace útoků, principy ACL a jejich implementace na směrovačích a ASA Základní zabezpečení ASA firewallu Konfigurace Zone-Based policy firewallu na směrovačích Základy IPS a jejich konfigurace na směrovačích s využitím CCP Typy a metody šifrování, implementace site-to-site VPN, IKEv2 IPv6 a IPsec, tunelovací metody, FIPS 140 suite B Implementace SSL VPN s využitím Cisco ASA</p>
EXAM 640-554 Implementing Cisco IOS Network Security	Zkouška Implementing Cisco IOS Network Security

<p>SISAS – Implementing Cisco Secure Access Solutions</p>	<p>Síťový koncept a komponenty nutné pro implementaci 802.1X IEEE 802.1X standard Autentizační protokol EAP Role RADIUS protokolu v 802.1X procesu Konfigurace síťové infrastruktury (suplikant, přepínač, WLC, ISE, operační systém) Konfigurace různých scénářů nasazení (MAB - MAC Authentication Bypass, webová autentizace, zařízení bez suplikanta, monitorovací režim, Low Impact) Guest Access, autorizace uživatelů, monitoring autentizovaných uživatelů Design 802.1X pomocí Cisco ISE, kritické scénáře v důsledku výpadk Seznámení s Cisco TrustSec 2.0 a ISE architekturou Možnosti nasazení Cisco Identity Services Engine - instalace Cisco ISE, konfigurace vysoké dostupnosti Cisco ISE Klasifikace a politiky - využití Cisco ISE pro vynucení politik, konfigurace Cisco ISE pro MAB (MAC Authentication Bypass), konfigurace Cisco ISE pro wired a wireless 802.1X autentizaci, nasazení ISE do VPN prostředí, nasazení ISE s Web autentizací Guest, Profiler a Posture služby Návrh Cisco TrustSec 2.0 architektury pro ISE</p>
<p>EXAM 300-208 Implementing Cisco Secure Access Solutions</p>	<p><u>Zkouška Implementing Cisco Secure Access Solutions</u></p>
<p>SIMOS – Implementing Cisco Secure Mobility Solutions</p>	<p>Popis různých VPN technologií a důvodů jejich nasazení. Používané šifrovací algoritmy a protokoly Implementace a troubleshooting Cisco site-to-site VPN řešení. Implementace Cisco FlexVPN: point-to-point, hub-and-spoke a spoke-to-spoke IPsec VPN. Implementace Cisco clientless SSL VPNs. Implementace Cisco AnyConnect SSL a IPsec VPNs. Implementace zabezpečení vzdáleného přístupu s vazbou na Dynamic Access Policies (DAP).</p>
<p>EXAM 300-209 Implementing Cisco Secure Mobility Solutions</p>	<p><u>Zkouška Implementing Cisco Secure Mobility Solutions</u></p>

<p>SENSS – Implementing Cisco Edge Network Security Solutions</p>	<p>Principy bezpečnostního design Bezpečnostní segmentace sítě Cisco modulární síťová architektura Cisco SecureX architektura Cisco TrustSec řešení Nasazení ochrany síťové infrastruktury Seznámení s Cisco Network Infrastructure Protection Nasazení Cisco IOS Control Plane Security Nasazení Cisco IOS Management Plane Security Nasazení Cisco ASA Management Plane Security Nasazení Cisco Traffic Telemetry metod Nasazení Cisco IOS Layer 2 Data Plane Security Nasazení Cisco Layer 3 Data Plane Security Nasazení NAT na Cisco IOS Software a Cisco ASA Seznámení s Network Address Translation Nasazení Cisco ASA Network Address Translation Nasazení Cisco IOS Software Network Address Translation Nasazení Threat Control funkcí na Cisco ASA Seznámení s Cisco Firewall Threat Controls Nasazení základních Cisco ASA přístupových politik Nasazení pokročilých Cisco ASA přístupových politik Nasazení Reputation-Based Cisco ASA přístupových politik Nasazení Identity-Based Cisco ASA přístupových politik Nasazení Threat Control funkcí na Cisco IOS Software Nasazení základních Cisco IOS Zone-Based Policy Firewall přístupových politik Nasazení pokročilých Cisco IOS Zone-Based Policy Firewall přístupových politik</p>
<p>EXAM 300-206 Implementing Cisco Edge Network Security Solutions</p>	<p>Zkouška Implementing Cisco Edge Network Security Solutions</p>

<p>SITCS – Implementing Cisco Threat Control Solutions</p>	<p>Cisco ASA (CX) NGFW služby Seznámení s Cisco ASA (CX) NGFW Popis Cisco ASA (CX) NGFW Management architektury Konfigurace Cisco ASA (CX) NGFW Monitoring Cisco ASA (CX) NGFW Cisco Web Security Appliance Seznámení s řešením Cisco Web Security Appliance Integrace Cisco Web Security Appliance Konfigurace Cisco Web Security Appliance Cisco Cloud Web Security Seznámení s řešením Cisco Cloud Web Security Konfigurace Cisco Cloud Web Security Connectors Popis web filtrovacích politik v Cisco ScanCenter Cisco Email Security Appliance Seznámení s řešením Cisco Email Security Popis Cisco Email Security Appliance - základní komponenty nastavení Konfigurace Cisco Email Security Appliance - základní příchozí a odchozí poštovní politiky Cisco Intrusion Prevention Systems Seznámení s řešením Cisco IPS Integrace Cisco IPS senzorů do sítě Základní konfigurace Cisco IPS Ladění Cisco IPS signatur Konfigurace vlastních Cisco IPS signatur Konfigurace Cisco IPS Anomaly Detection Konfigurace Cisco IPS reputačních funkcí</p>
<p>EXAM 300-207 Implementing Cisco Threat Control Solutions</p>	<p>Zkouška Implementing Cisco Threat Control Solutions</p>

<p>CIPTV1 – Implementing Cisco IP Telephony and Video, Part 1</p>	<p>Úvod do problematiky Cisco Unified Communications Manager Architektura a typické scénáře nasazení Možnosti redundance Instalace systému a prvotní konfigurace služeb Registrace koncových zařízení a konfigurace uživatelů Implementace číslovacího plánu pro tzv. Single-Site model Komponenty číslovacího plánu Adresace koncových zařízení Konfigurace oprávnění pro volání Manipulace s čísly Směrování hovorů do PSTN Popis protokolů MGCP/H.323/SIP Konfigurace hlasových bran Popis funkcionality CUBE (Cisco Unified Border Element) SIP trunk Multimediální zdroje CUCM Music On Hold Media Termination Point Audio/video konferenční služby Popis prvků využívaných pro konferenční hovory Cisco TelePresence Server Cisco TelePresence Conductor Cisco TelePresence MSE 8000 Problematika QoS v sítích s collaboration řešením Úvod do QoS Principy a komponenty QoS</p>
<p>EXAM 642 - 447 Implementing Cisco Unified Communications Manager, Part 1</p>	<p><u>Zkouška Implementing Cisco Unified Communications Manager</u></p>

<p>CIPTV2 – Implementing Cisco IP Telephony and Video, Part 2</p>	<p>CUCM v multi-site prostředí Scénáře nasazení a možnosti redundance Možné problémy nasazení Design a problematika číslovacího plánu Redundance signalizace a směrování hovorů Cisco Unified SRST MGCP fallback Správa dostupné přenosové kapacity WAN Implementace Call Admission Control Omezení počtu audio/video hovorů CUCM a funkce pro mobilitu uživatelů Konfigurace Device Mobility Konfigurace Cisco Extension Mobility Konfigurace Cisco Unified Mobility Cisco VCS and Cisco Expressway Popis prvků a architektura Preferovaný design s CUCM Konfigurace MRA (Mobile Remote Access) Služby pro automatizovanou distribuci informací v prostředí CUCM Popis a implementace ILS, GDPR, CCD</p>
<p>EXAM 642 - 457 Implementing Cisco Unified Communications Manager, Part 2</p>	<p><u>Zkouška Implementing Cisco Unified Communications Manager, part 2</u></p>
<p>CAPPS – Implementing Collaboration Applications</p>	<p>Nasazení Cisco Unity Connection (CUC) Popis produktu a scénáře nasazení (včetně redundance) Instalace a integrace s CUCM Nastavení základních parametrů systému Konfigurace šablon a uživatelů Řešení problémů s nasazením CUC Nasazení Cisco Unity Express (CUE) Popis produktu a scénáře nasazení Instalace a integrace s CUCM Nastavení základních parametrů systému Konfigurace šablon a uživatelů Řešení problémů s nasazením CUC Nasazení Cisco Unified IM and Presence a Cisco Jabber (Desktop a Mobile) Popis produktu a scénáře nasazení Integrace IM/P s CUCM Nastavení základních parametrů systému Nasazení SW klienta Cisco Jabber Cisco Jabber Service Discovery Integrace Cisco Jabber s adresářovými službami Řešení problémů s implementací IM/P a Jabber Cisco VCS and Cisco TM Popis produktů Instalace, integrace a řešení problémů</p>
<p>EXAM 642 - 467 Integrating Cisco Unified Communications Applications</p>	<p><u>Zkouška Integrating Cisco Unified Communications Application</u></p>

SPROUTE– Deploying Cisco Service Provider Network Routing	Seznámení se směrovacími protokoly používanými v sítích poskytovatelů služeb Implementace protokolu OSPF v síti poskytovatele služeb Implementace OSPF se speciálními typy oblastí Implementace integrated IS-IS protokolu v síti poskytovatele služeb Implementace IS-IS směrování Implementace BGP v síti poskytovatele služeb Implementace základního BGP směrování
SPADVROUTE-Deploying Cisco Service Provider Advanced Routing	Konektivita v sítích poskytovatelů služeb s využitím protokolu BGP Definice požadavků zákazníka na konektivitu s poskytovatelem služeb Připojení zákazníka k poskytovateli služeb Škálovatelnost v sítích poskytovatelů služeb Řešení škálovatelnosti protokolu BGP v sítích poskytovatelů služeb Seznámení s užitím BGP routereflektorů a BGP konfederace Bezpečnost a optimalizace BGP protokolu Implementace pokročilých funkcí v BGP Ladění BGP konvergence Škálovatelnost v konfiguraci BGP Úvod do IP Multicastu Úvod do IP Multicastu Definování Multicast distribučního stromu a forwarding multicast provozu Multicast v síti LAN Mroute tabulka a její naplnění Směrování Multicast provozu uvnitř domény a mezi doménami Úvod do PIM-SM protokolu Implementace a pokročilá konfigurace PIM-SM Implementace Interdomain IP multicast Řešení distribuce Rendezvous Pointů Metody přechodu na IPv6 v sítích poskytovatelů služeb. Úvod do protokolu IPv6 Seznámení se s přechodovými mechanismy na IPv6 Nasazení IPv6 v síti poskytovatele služeb

<p>SPCORE-Implementing Cisco SP Next-Generation Core Network Services</p>	<p>Multiprotocol Label Switching Seznámení s MPLS Spuštění Label Distribution Protocolu Implementace MPLS v páteři Service Provider sítě MPLS Traffic Engineering Seznámení s MPLS Traffic Engineering funkcionalitou Spuštění MPLS Traffic Engineeringu Implementace MPLS TE Ochrana MPLS TE provoz v případě poruchy (Fast Reroute) QoS v síti poskytovatele služeb Principy QoS Implementace Cisco QoS a QoS mechanismy Implementace MPLS a podpora QoS Klasifikace a značkování QoS Principy klasifikace třídění a značkování Použití Modularního QoS CLI (MQC) Implementace pokročilých QoS funkcí QoS řízení zahlcení Správa zahlcení Implementace správy zahlcení QoS Traffic Shaping a policing ČR Principy Traffic Shapingu a Policingu Implementace Policingu Implementace Traffic Shapingu</p>
<p>SPEDGE-Implementing Cisco SP Next-Generation Edge Network Services</p>	<p>VPN technologie MPLS Layer 3 VPN Implementace MPLS Layer 3 VPN páteře Připojení zákazníků s použitím jednoduchých směrovacích protokolů Připojení zákazníků pomocí BGP nebo OSPF IPv6 a MPLS Komplexní MPLS Layer 3 VPN Implementace komplexních MPLS Layer 3 VPN Implementace přístupu k internetu a MPLS Layer 3 VPN Seznámení s MPLS Inter-AS řešeními Layer 2 VPN a Ethernet Služby Seznámení s Layer 2 VPN Seznámení s funkcí Any Transport over MPLS Implementace VPLS</p>

Příloha č. 3 Oprávněné osoby

Za Objednatele:

ve věcech smluvních:

Jméno a příjmení	[REDACTED]
Adresa	Křížová 25, Praha 5, 225 08
E-mail	[REDACTED]
Telefon	[REDACTED]

ve věcech obchodních:

Jméno a příjmení	[REDACTED]
Adresa	Křížová 25, Praha 5, 225 08
E-mail	[REDACTED]
Telefon	[REDACTED]

ve věcech technických:

Jméno a příjmení	[REDACTED]
Adresa	Křížová 25, Praha 5, 225 08
E-mail	[REDACTED]
Telefon	[REDACTED]

ve věcech kybernetické bezpečnosti:

Jméno a příjmení	[REDACTED]
Adresa	Křížová 6A, Praha 5, 225 08
E-mail	[REDACTED]
Telefon	[REDACTED]

Za Poskytovatele:

ve věcech smluvních:

Jméno a příjmení	[REDACTED]
Adresa	Kladenská 1879/3, 160 00 Praha 6
E-mail	[REDACTED]
Telefon	[REDACTED]

ve věcech obchodních:

Jméno a příjmení	[REDACTED]
Adresa	Kladenská 1879/3, 160 00 Praha 6
E-mail	[REDACTED]
Telefon	[REDACTED]

ve věcech technických:


Jméno a příjmení	[REDACTED]
Adresa	Kladenská 1879/3, 160 00 Praha 6
E-mail	[REDACTED]
Telefon	[REDACTED]

ve věcech kybernetické bezpečnosti:

Jméno a příjmení	[REDACTED]
Adresa	Kladenská 1879/3, 160 00 Praha 6
E-mail	[REDACTED]
Telefon	[REDACTED]

Příloha č. 4 Seznam poddodavatelů

1)

Název:	ALEF NULA a.s.
Sídlo:	Pernerova 691/42, Karlín, 186 00 Praha 8
Právní forma:	akciová společnost
Identifikační číslo:	61858579
Rozsah plnění Smlouvy:	školení, poskytování servisu, expertní podpora
Kontaktní údaje:	
Procentuální podíl na plnění VZ:	18%

Poddodavatel prokazuje chybějící část technické kvalifikace.

Příloha č. 5 Specifikace ceny

Zařízení	Part Number	Cena Zařízení včetně Podpory	Maximální počet kusů Zařízení	Cena za maximální počet kusů Zařízení včetně Podpory	Cena za maximální počet kusů Zařízení včetně Podpory
	(který splňuje požadované funkcionality)	(bez DPH)	(ks)	(bez DPH)	(s DPH)
Prvek_A	C9300-48P-E	143 804,00 Kč	220	31 636 880,00 Kč	38 280 624,80 Kč
Modul_A1	PWR-C1- 1100WAC=	16 872,00 Kč	50	843 600,00 Kč	1 020 756,00 Kč
Modul_A2	C9300-NM-2Q=	22 644,00 Kč	20	452 880,00 Kč	547 984,80 Kč
Modul_A3	C9300-NM-2Y=	22 644,00 Kč	50	1 132 200,00 Kč	1 369 962,00 Kč
Modul_A4	C9300-NM-8X=	22 644,00 Kč	60	1 358 640,00 Kč	1 643 954,40 Kč
Modul_A5	C9300-NM-4M=	13 320,00 Kč	50	666 000,00 Kč	805 860,00 Kč
Modul_A6	STACK-T1-1M=	2 051,00 Kč	130	266 630,00 Kč	322 622,30 Kč
Modul_A7	STACK-T1-3M=	3 076,00 Kč	50	153 800,00 Kč	186 098,00 Kč
Modul_A8	CAB-SPWR- 150CM=	1 911,00 Kč	130	248 430,00 Kč	300 600,30 Kč
Modul_A9	C9300-48-E-A-3	38 001,00 Kč	220	8 360 220,00 Kč	10 115 866,20 Kč
Prvek_B	WS-C2960X- 48LPS-L	70 871,00 Kč	10	708 710,00 Kč	857 539,10 Kč
Modul_B1	CAB-STK-E-0.5M	12 210,00 Kč	10	122 100,00 Kč	147 741,00 Kč
Modul_B2	C2960X-HYBRID- STK=	12 210,00 Kč	10	122 100,00 Kč	147 741,00 Kč
Modul_B3	C2960X-FIBER- STK=	12 210,00 Kč	10	122 100,00 Kč	147 741,00 Kč
Modul_B4	CAB-STK-E-0.5M=	888,00 Kč	10	8 880,00 Kč	10 744,80 Kč
Modul_B5	CAB-STK-E-1M=	1 776,00 Kč	10	17 760,00 Kč	21 489,60 Kč
Modul_B6	CAB-STK-E-3M=	2 937,00 Kč	10	29 370,00 Kč	35 537,70 Kč
Prvek_C	WS-C3650-48PS-S	137 918,00 Kč	4	551 672,00 Kč	667 523,12 Kč
Modul_C1	PWR-C2- 640WAC=	10 656,00 Kč	4	42 624,00 Kč	51 575,04 Kč
Modul_C2	PWR-C2- 1025WAC=	15 984,00 Kč	4	63 936,00 Kč	77 362,56 Kč
Modul_C3	C3650-STACK- KIT=	16 872,00 Kč	4	67 488,00 Kč	81 660,48 Kč
Modul_C4	STACK-T2-50CM=	1 243,20 Kč	4	4 972,80 Kč	6 017,09 Kč
Modul_C5	STACK-T2-1M=	2 308,00 Kč	4	9 232,00 Kč	11 170,72 Kč
Modul_C6	STACK-T2-3M=	3 463,00 Kč	4	13 852,00 Kč	16 760,92 Kč
Modul_C7	L-C3650-48-S-E	89 421,00 Kč	4	357 684,00 Kč	432 797,64 Kč
Prvek_D	WS-C3850-12XS-S	209 660,00 Kč	2	419 320,00 Kč	507 377,20 Kč
Modul_D1	C3850-NM-4-10G=	48 040,00 Kč	2	96 080,00 Kč	116 256,80 Kč
Modul_D2	PWR-C1- 350WAC=	5 772,00 Kč	2	11 544,00 Kč	13 968,24 Kč
Modul_D3	L-C3850-12-S-E	30 103,00 Kč	2	60 206,00 Kč	72 849,26 Kč
Prvek_E	C9200L-24P-4G-E	48 837,00 Kč	30	1 465 110,00 Kč	1 772 783,10 Kč
Modul_E1	STACK-T4-1M=	1 776,00 Kč	10	17 760,00 Kč	21 489,60 Kč
Modul_E2	STACK-T4-3M=	2 664,00 Kč	10	26 640,00 Kč	32 234,40 Kč
Modul_E3	C9200L-24-E-A-3	20 260,00 Kč	30	607 800,00 Kč	735 438,00 Kč
Prvek_F	C9407R-96U- BNDL-E	297 757,00 Kč	23	6 848 411,00 Kč	8 286 577,31 Kč
Modul_F1	C9400-DNA-E-A-3	129 528,00 Kč	23	2 979 144,00 Kč	3 604 764,24 Kč
Modul_F2	C9400-SUP-1=	181 152,00 Kč	23	4 166 496,00 Kč	5 041 460,16 Kč

Modul_F3	C9400-LC-48T=	63 403,00 Kč	23	1 458 269,00 Kč	1 764 505,49 Kč
Modul_F4	C9400-LC-48P=	66 600,00 Kč	46	3 063 600,00 Kč	3 706 956,00 Kč
Modul_F5	C9400-LC-48UX=	102 120,00 Kč	23	2 348 760,00 Kč	2 841 999,60 Kč
Modul_F6	C9400-LC-24S=	124 320,00 Kč	2	248 640,00 Kč	300 854,40 Kč
Modul_F7	C9400-LC-48S=	222 000,00 Kč	2	444 000,00 Kč	537 240,00 Kč
Modul_F8	C9400-LC-24XS=	217 382,00 Kč	2	434 764,00 Kč	526 064,44 Kč
Modul_F9	C9400-PWR-3200AC=	18 115,00 Kč	5	90 575,00 Kč	109 595,75 Kč
Modul_F10	C9400-PWR-2100AC=	18 115,00 Kč	5	90 575,00 Kč	109 595,75 Kč
Prvek_G	C9500-24Y4C-A	338 675,00 Kč	6	2 032 050,00 Kč	2 458 780,50 Kč
Prvek_H	C9407R	510 078,00 Kč	4	2 040 312,00 Kč	2 468 777,52 Kč
Modul_H1	C9400-SUP-1XL=	226 440,00 Kč	4	905 760,00 Kč	1 095 969,60 Kč
Modul_H2	C9400-LC-24XS=	217 382,00 Kč	10	2 173 820,00 Kč	2 630 322,20 Kč
Modul_H3	C9400-LC-48S=	222 000,00 Kč	4	888 000,00 Kč	1 074 480,00 Kč
Modul_H4	C9400-LC-24S=	124 320,00 Kč	4	497 280,00 Kč	601 708,80 Kč
Modul_H5	C9400-LC-48UX=	102 120,00 Kč	4	408 480,00 Kč	494 260,80 Kč
Modul_H6	C9400-LC-48T=	63 403,00 Kč	6	380 418,00 Kč	460 305,78 Kč
Prvek_I	C9200L-48P-4G-E	87 822,00 Kč	360	31 615 920,00 Kč	38 255 263,20 Kč
Modul_I1	STACK-T4-1M=	1 776,00 Kč	100	177 600,00 Kč	214 896,00 Kč
Modul_I2	STACK-T4-3M=	2 664,00 Kč	20	53 280,00 Kč	64 468,80 Kč
Modul_I3	C9200L-48-E-A-3	38 001,00 Kč	360	13 680 360,00 Kč	16 553 235,60 Kč
Prvek_J	WS-C3560CX-12PD-S	27 212,00 Kč	20	544 240,00 Kč	658 530,40 Kč
Prvek_K	C9200-48P-E	96 820,00 Kč	20	1 936 400,00 Kč	2 343 044,00 Kč
Modul_K1	C9200-NM-4X=	17 760,00 Kč	15	266 400,00 Kč	322 344,00 Kč
Modul_K2	C9200-NM-4G=	4 528,00 Kč	10	45 280,00 Kč	54 788,80 Kč
Modul_K3	STACK-T4-1M=	1 776,00 Kč	10	17 760,00 Kč	21 489,60 Kč
Modul_K4	STACK-T4-3M=	2 664,00 Kč	5	13 320,00 Kč	16 117,20 Kč
Modul_K5	C9200-48-E-A-3	38 001,00 Kč	20	760 020,00 Kč	919 624,20 Kč
Prvek_L	DN2-HW-APL	977 636,00 Kč	3	2 932 908,00 Kč	3 548 818,68 Kč
Prvek_M	C9120AXI-E	17 085,00 Kč	90	1 537 650,00 Kč	1 860 556,50 Kč
Prvek_N	C9120AXE-E	18 093,00 Kč	10	180 930,00 Kč	218 925,30 Kč
Modul_N1	AIR-ANT2524DW-R	453,00 Kč	40	18 120,00 Kč	21 925,20 Kč
Prvek_O	C9800-40-K9	602 716,00 Kč	2	1 205 432,00 Kč	1 458 572,72 Kč
Modul_O1	AIR-DNA	6 048,00 Kč	150	907 200,00 Kč	1 097 712,00 Kč
Prvek_P	DNAS-ACT	7 257,00 Kč	150	1 088 550,00 Kč	1 317 145,50 Kč
Prvek_Q	N9K-C9332C	381 322,00 Kč	4	1 525 288,00 Kč	1 845 598,48 Kč
Prvek_R	N9K-C93180YC-FX	385 311,00 Kč	4	1 541 244,00 Kč	1 864 905,24 Kč
Prvek_S	N9K-C93240YC-FX2	490 393,00 Kč	8	3 923 144,00 Kč	4 747 004,24 Kč
Prvek_T	N77-C7706-B33S3E	1 660 538,00 Kč	2	3 321 076,00 Kč	4 018 501,96 Kč
Modul_T1	N77-F312CK-26=	734 400,00 Kč	2	1 468 800,00 Kč	1 777 248,00 Kč
Modul_T2	N77-F324FQ-25=	448 800,00 Kč	2	897 600,00 Kč	1 086 096,00 Kč
Modul_T3	N77-F348XP-23=	359 040,00 Kč	2	718 080,00 Kč	868 876,80 Kč
Prvek_U	APIC-M3	230 968,00 Kč	6	1 385 808,00 Kč	1 676 827,68 Kč
Prvek_V	APIC-L3	319 706,00 Kč	6	1 918 236,00 Kč	2 321 065,56 Kč
Prvek_W	FPR4140-NGFW-K9	2 325 616,00 Kč	8	18 604 928,00 Kč	22 511 962,88 Kč

Modul_W 1	FPR4K-NM- 4X40G=	885 924,00 Kč	1	885 924,00 Kč	1 071 968,04 Kč
Modul_W 2	L-AC-PLS-3Y-S6	70 668,00 Kč	1	70 668,00 Kč	85 508,28 Kč
Modul_W 3	L-AC-APX-3Y-S6	172 224,00 Kč	1	172 224,00 Kč	208 391,04 Kč
Prvek_X	FMC1600-K9	329 480,00 Kč	1	329 480,00 Kč	398 670,80 Kč
Prvek_Y	WSA-S695F-K9	500 918,00 Kč	2	1 001 836,00 Kč	1 212 221,56 Kč
Modul_Y1	WSA-WSP-LIC	4 352 400,00 Kč	1	4 352 400,00 Kč	5 266 404,00 Kč
Modul_Y2	WSA-AMP-LIC	2 732 184,00 Kč	1	2 732 184,00 Kč	3 305 942,64 Kč
Prvek_Z	ESA-C695F-K9	373 326,00 Kč	2	746 652,00 Kč	903 448,92 Kč
Modul_Z1	ESA-ESP-LIC	5 068 440,00 Kč	1	5 068 440,00 Kč	6 132 812,40 Kč
Modul_Z2	ESA-AMP-LIC	3 316 248,00 Kč	1	3 316 248,00 Kč	4 012 660,08 Kč
Prvek_AA	SMA-M695F-K9	396 087,00 Kč	2	792 174,00 Kč	958 530,54 Kč
Modul_AA 1	SMA-EMGT-LIC	379 080,00 Kč	1	379 080,00 Kč	458 686,80 Kč
Modul_AA 2	SMA-WMGT-LIC	182 520,00 Kč	1	182 520,00 Kč	220 849,20 Kč
Prvek_AB	L-ISE-BSE-PLIC	4 896,00 Kč	1	4 896,00 Kč	5 924,16 Kč
Modul_AB 1	SNS-3655-K9	480 245,00 Kč	2	960 490,00 Kč	1 162 192,90 Kč
Modul_AB 2	L-ISE-BSE-P7	240 883,00 Kč	1	240 883,00 Kč	291 468,43 Kč
Modul_AB 3	L-ISE-PLS-3Y-S7	1 223 352,00 Kč	1	1 223 352,00 Kč	1 480 255,92 Kč
Modul_AB 4	L-ISE-APX-3Y-S6	463 320,00 Kč	1	463 320,00 Kč	560 617,20 Kč
Modul_AB 5	L-ISE-TACACS- ND=	163 200,00 Kč	2	326 400,00 Kč	394 944,00 Kč
Prvek_AC	AMP4E-ADV-CL- LIC	1 061,00 Kč	10000	10 610 000,00 Kč	12 838 100,00 Kč
Modul_AD 1	SFP-H10GB- CU1M=	816,00 Kč	100	81 600,00 Kč	98 736,00 Kč
Modul_AD 2	SFP-H10GB-CU1- 5M=	816,00 Kč	100	81 600,00 Kč	98 736,00 Kč
Modul_AD 3	SFP-H10GB- CU2M=	816,00 Kč	100	81 600,00 Kč	98 736,00 Kč
Modul_AD 4	SFP-H10GB-CU2- 5M=	816,00 Kč	100	81 600,00 Kč	98 736,00 Kč
Modul_AD 5	SFP-H10GB- CU3M=	816,00 Kč	100	81 600,00 Kč	98 736,00 Kč
Modul_AD 6	SFP-H10GB- CU5M=	1 224,00 Kč	100	122 400,00 Kč	148 104,00 Kč
Modul_AD 7	SFP-H10GB- ACU7M=	2 937,00 Kč	50	146 850,00 Kč	177 688,50 Kč
Modul_AD 8	SFP-H10GB- ACU10M=	3 345,00 Kč	50	167 250,00 Kč	202 372,50 Kč
Modul_AD 9	SFP-10G-AOC1M=	1 713,00 Kč	100	171 300,00 Kč	207 273,00 Kč
Modul_AD 10	SFP-10G-AOC2M=	1 713,00 Kč	100	171 300,00 Kč	207 273,00 Kč
Modul_AD 11	SFP-10G-AOC3M=	1 713,00 Kč	100	171 300,00 Kč	207 273,00 Kč
Modul_AD	SFP-10G-AOC5M=	2 121,00 Kč	100	212 100,00 Kč	256 641,00 Kč

12					
Modul_AD 13	SFP-10G-AOC7M=	2 121,00 Kč	50	106 050,00 Kč	128 320,50 Kč
Modul_AD 14	SFP-10G-AOC10M=	2 121,00 Kč	50	106 050,00 Kč	128 320,50 Kč
Modul_AD 15	SFP-10G-SR-S=	5 712,00 Kč	100	571 200,00 Kč	691 152,00 Kč
Modul_AD 16	SFP-10G-LR-S=	16 320,00 Kč	20	326 400,00 Kč	394 944,00 Kč
Modul_AD 17	SFP-10G-LRM=	8 976,00 Kč	100	897 600,00 Kč	1 086 096,00 Kč
Modul_AD 18	SFP-10G-ER-S=	64 464,00 Kč	8	515 712,00 Kč	624 011,52 Kč
Modul_AD 19	SFP-10G-ZR-S=	88 944,00 Kč	4	355 776,00 Kč	430 488,96 Kč
Modul_AD 20	SFP-10G-BXD-I=	42 432,00 Kč	4	169 728,00 Kč	205 370,88 Kč
Modul_AD 21	SFP-10G-BXU-I=	42 432,00 Kč	4	169 728,00 Kč	205 370,88 Kč
Modul_AD 22	GLC-TE=	3 672,00 Kč	100	367 200,00 Kč	444 312,00 Kč
Modul_AD 23	GLC-SX-MMD=	4 080,00 Kč	100	408 000,00 Kč	493 680,00 Kč
Modul_AD 24	GLC-LH-SMD=	8 119,00 Kč	50	405 950,00 Kč	491 199,50 Kč
Modul_AD 25	GLC-ZX-SMD=	32 599,00 Kč	4	130 396,00 Kč	157 779,16 Kč
Modul_AD 26	QSFP-40G-SR-BD=	8 935,00 Kč	40	357 400,00 Kč	432 454,00 Kč
Modul_AD 27	QSFP-40G-LR4-S=	88 944,00 Kč	4	355 776,00 Kč	430 488,96 Kč
Modul_AD 28	QSFP-H40G-CU1M=	2 040,00 Kč	30	61 200,00 Kč	74 052,00 Kč
Modul_AD 29	QSFP-H40G-CU3M=	2 040,00 Kč	30	61 200,00 Kč	74 052,00 Kč
Modul_AD 30	QSFP-H40G-CU5M=	3 060,00 Kč	30	91 800,00 Kč	111 078,00 Kč
Modul_AD 31	QSFP-H40G-ACU7M=	8 976,00 Kč	10	89 760,00 Kč	108 609,60 Kč
Modul_AD 32	QSFP-H40G-ACU10M=	10 200,00 Kč	10	102 000,00 Kč	123 420,00 Kč
Modul_AD 33	QSFP-H40G-AOC1M=	6 936,00 Kč	20	138 720,00 Kč	167 851,20 Kč
Modul_AD 34	QSFP-H40G-AOC2M=	6 936,00 Kč	20	138 720,00 Kč	167 851,20 Kč
Modul_AD 35	QSFP-H40G-AOC3M=	6 936,00 Kč	20	138 720,00 Kč	167 851,20 Kč
Modul_AD 36	QSFP-H40G-AOC5M=	8 160,00 Kč	20	163 200,00 Kč	197 472,00 Kč
Modul_AD 37	QSFP-H40G-AOC7M=	8 160,00 Kč	10	81 600,00 Kč	98 736,00 Kč
Modul_AD 38	QSFP-H40G-AOC10M=	8 160,00 Kč	10	81 600,00 Kč	98 736,00 Kč
Modul_AD 39	QSFP-H40G-AOC15M=	9 792,00 Kč	4	39 168,00 Kč	47 393,28 Kč

Modul_AD 40	DS-SFP-FC8G- SW=	2 121,00 Kč	20	42 420,00 Kč	51 328,20 Kč
Modul_AD 41	DS-SFP-FC8G- LW=	17 707,00 Kč	4	70 828,00 Kč	85 701,88 Kč
Prvek_AE	UCSC-C220-M5SX	174 975,00 Kč	6	1 049 850,00 Kč	1 270 318,50 Kč
Prvek_AF	ISR4331-SEC/K9	98 676,00 Kč	4	394 704,00 Kč	477 591,84 Kč
Prvek_AG	UCS-E160S- M3/K9=_1	73 691,00 Kč	2	147 382,00 Kč	178 332,22 Kč
Prvek_AH	UCS-E160S- M3/K9=_2	73 691,00 Kč	2	147 382,00 Kč	178 332,22 Kč
Prvek_AI	UCS-E160S- M3/K9=_3	145 619,00 Kč	2	291 238,00 Kč	352 397,98 Kč
Prvek_AJ	UCS-E160S- M3/K9=_4	145 619,00 Kč	2	291 238,00 Kč	352 397,98 Kč
Prvek_AK	UCS-E160S- M3/K9=_5	315 731,00 Kč	1	315 731,00 Kč	382 034,51 Kč
Prvek_AL	ASR1001-X	711 643,00 Kč	1	711 643,00 Kč	861 088,03 Kč
Prvek_AM	ASR1002-HX	2 051 520,00 Kč	2	4 103 040,00 Kč	4 964 678,40 Kč
Modul_A M1	FLSA1-HX-2X1GE=	17 864,00 Kč	4	71 456,00 Kč	86 461,76 Kč
Modul_A M2	FLSA1-HX- 2X10GE=	166 715,00 Kč	4	666 860,00 Kč	806 900,60 Kč
Modul_A M3	FLSA1- MACSEC1G=	10 433,00 Kč	8	83 464,00 Kč	100 991,44 Kč
Modul_A M4	FLSA1- MACSEC10G=	73 718,00 Kč	8	589 744,00 Kč	713 590,24 Kč
Modul_A M5	EPA-1X40GE=	454 092,00 Kč	2	908 184,00 Kč	1 098 902,64 Kč
Modul_A M6	EPA-2X40GE=	697 005,00 Kč	2	1 394 010,00 Kč	1 686 752,10 Kč
Modul_A M7	FLSA1- 2HX8G16G=	294 910,00 Kč	2	589 820,00 Kč	713 682,20 Kč
Modul_A M8	FLSA1- 2HX8G25G=	491 505,00 Kč	2	983 010,00 Kč	1 189 442,10 Kč
Prvek_AN	CS-BOARD55S-G- K9	541 756,00 Kč	4	2 167 024,00 Kč	2 622 099,04 Kč
Prvek_AO	CS-BOARD85S-G- K9	1 557 117,00 Kč	1	1 557 117,00 Kč	1 884 111,57 Kč
Prvek_AP	CS-KIT-K9	229 195,00 Kč	5	1 145 975,00 Kč	1 386 629,75 Kč
Prvek_AQ	CS-KIT-MINI-K9	118 881,00 Kč	1	118 881,00 Kč	143 846,01 Kč
Prvek_AR	CS-ROOM55-K9	528 004,00 Kč	1	528 004,00 Kč	638 884,84 Kč
Prvek_AS	CTI-CMS1KM5- BUN-K9	1 276 104,00 Kč	1	1 276 104,00 Kč	1 544 085,84 Kč
Celková cena za Zařízení, vč. Podpory				235 356 582,80 Kč	284 781 465,19 Kč

Školení	Cena za 1 osobu	Maximální počet osob	Cena za maximální počet osob	Cena za maximální počet osob
	(bez DPH)	(ks)	(bez DPH)	(s DPH)
ICND1 – Interconnecting Cisco Networking Devices Part 1	8 211,00 Kč	6	49 266,00 Kč	59 611,86 Kč
ICND2 – Interconnecting Cisco Networking Devices Part 2	8 211,00 Kč	6	49 266,00 Kč	59 611,86 Kč
EXAM 200 - 125 CCNA Cisco Certified Network Associate (803)	2 730,00 Kč	6	16 380,00 Kč	19 819,80 Kč
ROUTE – IMPLEMENTING CISCO IP ROUTING	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
EXAM 300-101 IMPLEMENTING CISCO IP ROUTING	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
SWITCH – IMPLEMENTING CISCO IP SWITCHED NETWORKS	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
EXAM 300-115 - IMPLEMENTING CISCO IP SWITCHED NETWORKS	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
DESGN – DESIGNING FOR CISCO INTERNETWORK SOLUTIONS	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
EXAM 640 - 864 DESIGNING FOR CISCO INTERNETWORK SOLUTIONS	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
TSHOOT – TROUBLESHOOTING AND MAINT. CISCO IP NETWORKS	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
EXAM 300-135 TROUBLESHOOTING AND MAINTAINING CISCO IP NETWORKS	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
ARCH – DESIGNING CISCO NETWORK SERVICES ARCHITECTURE	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
EXAM 642 - 874 DESIGNING CISCO NETWORK SERVICE ARCHITECTURES	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
DCNX1K – Implementing the Cisco Nexus 1000V	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
DCNX5K – Configuring Cisco Nexus 5000 Switches	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
DCID školení	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
DCII školení	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
DCUCI školení	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
DCVAI školení	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
DCIT školení	22 500,00 Kč	6	135 000,00 Kč	163 350,00 Kč
IINS – Implementing Cisco IOS Network Security	14 340,00 Kč	6	86 040,00 Kč	104 108,40 Kč
EXAM 640-554 Implementing Cisco IOS Network Security	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
SISAS – Implementing Cisco Secure Access Solutions	20 970,00 Kč	6	125 820,00 Kč	152 242,20 Kč

EXAM 300-208 Implementing Cisco Secure Access Solutions	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
SIMOS – Implementing Cisco Secure Mobility Solutions	20 970,00 Kč	6	125 820,00 Kč	152 242,20 Kč
EXAM 300-209 Implementing Cisco Secure Mobility Solutions	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
SENSS – Implementing Cisco Edge Network Security Solutions	20 970,00 Kč	6	125 820,00 Kč	152 242,20 Kč
EXAM 300-206 Implementing Cisco Edge Network Security Solutions	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
SITCS – Implementing Cisco Threat Control Solutions	20 970,00 Kč	6	125 820,00 Kč	152 242,20 Kč
EXAM 300-207 Implementing Cisco Threat Control Solutions	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
CIPTV1 – Implementing Cisco IP Telephony and Video, Part 1	22 200,00 Kč	6	133 200,00 Kč	161 172,00 Kč
EXAM 642 - 447 Implementing Cisco Unified Communications Manager, Part 1	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
CIPTV2 – Implementing Cisco IP Telephony and Video, Part 2	22 200,00 Kč	6	133 200,00 Kč	161 172,00 Kč
EXAM 642 - 457 Implementing Cisco Unified Communications Manager, Part 2	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
CAPPS – Implementing Collaboration Applications	23 970,00 Kč	6	143 820,00 Kč	174 022,20 Kč
EXAM 642 - 467 Integrating Cisco Unified Communications Applications	2 580,00 Kč	6	15 480,00 Kč	18 730,80 Kč
SPROUTE– Deploying Cisco Service Provider Network Routing	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
SPADVROUTE-Deploying Cisco Service Provider Advanced Routing	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
SPCORE-Implementing Cisco SP Next-Generation Core Network Services	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
SPEDGE-Implementing Cisco SP Next-Generation Edge Network Services	19 500,00 Kč	6	117 000,00 Kč	141 570,00 Kč
		Školení celkem	3 313 692,00 Kč	4 009 567,32 Kč

Položka	cena bez DPH	cena s DPH
Celková cena za Zařízení, vč. Podpory	235 356 582,80 Kč	284 781 465,19 Kč
Školení celkem	3 313 692,00 Kč	4 009 567,32 Kč
Cena celkem	238 670 274,80 Kč	288 791 032,51 Kč

Příloha č. 6 Realizační tým

Člen realizačního týmu	Kontaktní údaje
Vedoucí technik	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Vedoucí technik	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Projektový manažer	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Školitel	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Školitel	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Školitel	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Školitel	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Specialista v oblasti "Routing and Switching" síťové infrastruktury	Jméno a příjmení: ██████████ Telefon: ██████████ E-mail: ██████████
Specialista v oblasti "Security" síťové infrastruktury	Jméno a příjmení: ██████████ Telefon: ██████████

	E-mail: [REDACTED]
Specialista v oblasti "Voice" komunikační infrastruktury	Jméno a příjmení: [REDACTED] Telefon: [REDACTED] E-mail: [REDACTED]
Specialista v oblasti "Wireless" komunikační infrastruktury	Jméno a příjmení: [REDACTED] Telefon: [REDACTED] E-mail: [REDACTED]

Příloha č. 7 Vzor Dílčí smlouvy

Dílčí smlouva č. [BUDE DOPLNĚNO]

uzavřená na základě Rámcové smlouvy na dodávku aktivních prvků a rozšiřujících modulů
ze dne (dále jen „Rámcová smlouva“)

OBJEDNATEL : ČR - Česká správa sociálního zabezpečení
se sídlem : Křížová 1292/25, 225 08 Praha 5
IČO : 00006963
bankovní spojení : Česká národní banka
číslo účtu : 10006-127001/0710
jednající : [BUDE DOPLNĚNO]

POSKYTOVATEL : [BUDE DOPLNĚNO]
se sídlem : [BUDE DOPLNĚNO]
IČO : [BUDE DOPLNĚNO]
DIČ : [BUDE DOPLNĚNO]
bankovní spojení : [BUDE DOPLNĚNO]
číslo účtu : [BUDE DOPLNĚNO]
zastoupený : [BUDE DOPLNĚNO]

písemná výzva k poskytnutí plnění

Objednatel touto dílčí smlouvou vyzývá poskytovatele k plnění na základě výše uvedené Rámcové smlouvy; předmětem dílčí smlouvy je **dodávka zařízení včetně podpory dle katalogových listů (dále také jen „zařízení“), v počtech dle níže uvedené tabulky / poskytnutí školení specifikovaného níže** v celkové ceně [BUDE DOPLNĚNO] Kč bez DPH, sazba DPH 21%, tedy [BUDE DOPLNĚNO] Kč s DPH.

Objednatel vyzývá poskytovatele k **dodávce následujících zařízení / poskytnutí následujícího školení:**

katalogový list zařízení/ název školení	počet zařízení / počet osob	cena za 1 zařízení / 1 osobu bez DPH	cena celkem bez DPH	cena celkem s DPH
---	-----------------------------------	---	---------------------	-------------------

			Celkem	

Poskytovatel **odá zařzení do sídla objednatele na adresu Křížová 1292/25, 225 08 Praha 5, do 8 týdnů od nabytí účinnosti této dílčí smlouvy / poskytne školení v termínu [BUDE DOPLNĚNO] a místě [BUDE DOPLNĚNO].**

Poskytovatel souhlasí s tím, aby tato dílčí smlouva byla objednatelem uveřejněna v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

Tato dílčí smlouva nabývá platnosti ke dni jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění objednatelem v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), nebo ke dni, kdy bude poskytovateli ze strany objednatele doručeno oznámení, že objednateli bylo schváleno Stanovení výdajů financování akce ze státního rozpočtu ze strany příslušného správce rozpočtové kapitoly, tedy ze strany Ministerstva práce a sociálních věcí, a to dle toho, který z těchto okamžiků nastane později. Nedojde-li k tomuto Stanovení výdajů na financování předmětné akce, a to ani do 120 kalendářních dnů od dne nabytí platnosti dílčí smlouvy, dílčí smlouva se od svého počátku ruší. Smluvní strany nejsou v takovém případě povinny hradit si navzájem účelně vynaložené náklady a prohlašují, že mezi stranami neexistují žádné závazky a/nebo nároky, jejichž splnění by mohla druhá smluvní strana požadovat.

Česká republika

[BUDE DOPLNĚNO]

– Česká správa sociálního zabezpečení

V Praze dne: _____

V _____ dne: _____

[BUDE DOPLNĚNO]

[BUDE DOPLNĚNO]

Příloha č. 8 Seznam standardů ČSSZ

Číslo	Název souboru	Název dokumentu	Verze
1.	std_db_20200124_v0.98.pdf	Standard databází Oracle	0.98
2.	std_inet_1_12.doc	Standard připojení k Internetu	1.12
3.	std_pošta_1_01.pdf	Standard poštovního systému ČSSZ	1.01
4.	std_AD_DNS_DHCP_NTP_2.05.pdf	Standard AD DNS DHCP	2.05
5.	std_AVO1_11.doc	Standard Antivirové ochrany	1.11
6.	Standard systémové konfigurace pracovní stanice 3.00	Standard systémové konfigurace pracovní stanice	3.00
7.	std_metodikavyvoje_1_0_21.pdf	Standard metodiky vývoje	1_0_21
8.	std_pravidlareleasemanagementu_apv_1_2_7.pdf	Standard Release managementu	1_2_7
9.	std_net_2.0.pdf	Standard síťové infrastruktury	2.0
10.	Programátorské konvence.NET 2.0 - 4.5_v1_0_19.pdf	Programátorské konvence.NET	1_0_19
11.	BizTalkDevelopmentStandard.v2.01.pdf	Standard pro tvorbu aplikací pro Microsoft BizTalk server	2.01
12.	AAA_Pozadavky_na_aplikace_v9.04	Požadavky na nové aplikace při integraci do AAA portálu	9.04
13.	Standard_pro_tvorbu_skriptu_db_Oracle_0.5.pdf	Standard pro tvorbu, předávání a spouštění skriptů v databázích Oracle	0.5
14.	Standard API rozhraní systému DMA_CSSZ_DMS_WS_API_DMA_v4_3	API ROZHRANÍ SYSTÉMU DMA: WS_API_DMA - Standard rozhraní pro ukládání dokumentů do DMS	4.3
15.	CSSZ_DU_STD_V_1.13.pdf	Standard provozu databáze Oracle	1.13
16.	std_srv_0.42.pdf	Standard systémové konfigurace aplikačních serverů verze	0.42
17.	std_PKI_v2.pdf	Standard pro PKI	2.0
18.	Standard Komunikace SD s exter firm v1_00	Standard komunikace Servicedesku s externími firmami	1.00
19.	Std provoz prostředí v4	Standard provozních prostředí v prostředí IKT ČSSZ.docx	4.00
20.	Std SQL Serverů v0.01.pdf	Provozní standard SQL Serverů	0.01

S6.1.	Standard Přípravenost IIS ČSSZ na otevřená data.pdf	Standard Přípravenost IIS ČSSZ na otevřená data	0.4
S6.2.	Standard Tvorba IRI RDF zdrojů.pdf	Standard Tvorba IRI RDF zdrojů	0.2
S6.3.	Standard Využívání KE.pdf	Standard využívání kmenových evidencí	0.4
S6.4.	Standard Využívání datového katalogu.pdf	Standard využívání datového katalogu	0.5
S6.5.	Standard Číselníky ČSSZ.pdf	Standard Číselníky ČSSZ	0.5