[redacted]

Smlouva o dodávce systému č. 2018/0876

Smluvní strany

Kupující

Název/ obchodní firma:	Univerzita Karlova, Filozofická fakulta
Sídlo:	Náměstí Jana Palacha 2, 116 38 Praha 1
Korespondenční adresa:	Náměstí Jana Palacha 2, 116 38 Praha 1
zastoupená:	doc. PhDr. Michal Pullmann, Ph.D., děkan
IČO:	00216208
DIČ:	CZ00216208

společnost zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 75521.

(dále jen „kupující")

a

Prodávající

Název/obchodní firma:	Networksys a.s.
Sídlo:	Plzeňská 1567/182, 150 00 Praha 5
Korespondenční adresa:	Plzeňská 1567/182, 150 00 Praha 5
IČO:	261 78 109
DIČ:	CZ26178109
Zastoupen:	Ing. Jan Šíp, statutární ředitel
Bankovní spojení: [redacted], číslo účtu:	[redacted]

společnost zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 6563

(dále jen „prodávající")

(dále společně také jako „smluvní strany" nebo jednotlivě jako „smluvní strana")

uzavřely níže uvedeného dne, měsíce a roku, v souladu s ustanovením § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník *(dále jen „občanský zákoník")*, tuto

k u p n í s m l o u v u
(dále jen „smlouva")

I.
Předmět smlouvy

Tato smlouva se uzavírá na základě výsledků výběrového řízení na dodávky, vyhlášeného kupujícím, jako zadavatelem, pod názvem **„UK FF – Pořízení ICT– část I"** *(dále jen „výběrové řízení" nebo „zakázka")* a v souladu se zadávací dokumentací a nabídkou prodávajícího podanou v rámci shora uvedeného výběrového řízení.

1. Touto smlouvou se prodávající zavazuje dodat a odevzdat za podmínek v ní sjednaných kupujícímu systém, blíže specifikované v Příloze č. 1 Technická specifikace (dále jen „Příloha č. 1"), a odevzdat jej za podmínek v ní sjednaných kupujícímu.

2. Kupující se zavazuje řádně a včas dodaný systém převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu stanoveném touto smlouvou.

II.
Specifikace předmětu plnění

1. Předmětem plnění této smlouvy je dodávka systému specifikovaného v čl. I odst. 2 této smlouvy v rámci veřejné zakázky a s tím spojených služeb.

2. Technická specifikace předmětu plnění je dána Přílohou č. 1 této smlouvy.

3. Součástí předmětu plnění dle této smlouvy jsou i veškeré doklady potřebné k převzetí a užívání předmětu plnění, potřebné licence (HW, SW), které budou již zahrnuty v nabídkové ceně a konzultace pro kupujícího formou fyzické přítomnosti zástupce prodávajícího na místě plnění. Prodávající prohlašuje, že předmět plnění splňuje veškeré podmínky stanovené právními předpisy k používání předmětu plnění, a že kupujícímu předal veškeré doklady potřebné k provozování předmětu plnění, za což kupujícímu odpovídá. Prodávající se zavazuje s dodávkou systému dle čl. II odst. 1 této smlouvy dodat kupujícímu kompletní návod k obsluze v českém jazyce, a to ve formě listinné, tak i elektronické na CD (návod k obsluze systému musí být podrobný).

4. Předmětem plnění dle této smlouvy je dále následná instalace systému, uvedení do provozu a vyzkoušení jeho plné funkčnosti, technické a aplikační zaškolení 3 uživatelů (zaměstnanců kupujícího) v místě plnění a v potřebném rozsahu, detailní seznámení s provozem a jeho podmínkami, v případě požadovaného SW potřebné licence a bezplatný servis po dobu celé záruční lhůty dle této smlouvy.

5. Prodávající potvrzuje, že jako odborník v dané oblasti podnikání je schopný realizovat předmět plnění v souladu s touto smlouvou, za celkovou kupní cenu uvedenou v čl. III. odst. 1 této smlouvy, a že si je vědom skutečnosti, že kupující má jednoznačný zájem na realizaci předmětu plnění ve sjednaném čase za dohodnutou kupní cenu a v kvalitě dle této smlouvy.

(vše dále jen jako „předmět plnění, dodávka či systém")

III.
Kupní cena a platební podmínky

Kupní cena předmětu plnění specifikovaného v ustanovení čl. II. této smlouvy je bez DPH a je stanovena ve výši 5 911 330,00 Kč.
DPH ve výši 21% činí 1 241 379,30 Kč.
Kupní cena systému včetně DPH činí 7 152 709,30 Kč.

1. Kupní cena je stanovena jako nejvýše přípustná a konečná a zahrnuje celý předmět plnění tak, jak je vymezen v čl. II této smlouvy. Kupní cena se může měnit pouze v případě změny daňových předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

2. Právo na zaplacení kupní ceny vzniká prodávajícímu řádným splněním jeho závazku v místě plnění dle čl. IV. odst. 1 této smlouvy a způsobem uvedeným v této smlouvě. Podkladem pro úhradu kupní ceny kupujícím je daňový doklad – faktura, která musí být vystavena prodávajícím. Součástí faktury bude kopie Přejímacího a instalačního protokolu. Splatnost faktury je 30 kalendářních dnů od jejího doručení kupujícímu.

3. Kupní cena se považuje za uhrazenou okamžikem připsání fakturované částky na účet prodávajícího.

4. Faktura musí obsahovat potřebné náležitosti daňového dokladu ve smyslu platného zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a musí obsahovat:
   a) označení daňového dokladu a jeho pořadové číslo
   b) identifikační údaje kupujícího
   c) identifikační údaje prodávajícího
   d) označení banky a číslo účtu, na který má být úhrada provedena
   e) popis plnění
   f) datum vystavení a odeslání faktury
   g) datum uskutečnění zdanitelného plnění
   h) datum splatnosti
   i) výši částky bez DPH, výši DPH a částku celkem s DPH
   j) podpis, v případě elektronického odeslání jméno osoby, která fakturu vystavila
   k) název projektu, reg. č. projektu
   l) text "Tento projekt je spolufinancován Evropskou unií – Evropským fondem pro regionální rozvoj v rámci Operačního programu Podnikání a inovace pro konkurenceschopnost"

5. Kupující je oprávněn před uplynutím lhůty splatnosti faktury vrátit bez zaplacení fakturu, která neobsahuje náležitosti stanovené touto smlouvou nebo budou-li tyto údaje uvedeny chybně. Prodávající je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. V takovém případě není kupující v prodlení se zaplacením ceny systému. Okamžikem doručení náležitě doplněné či opravené faktury začne běžet nová lhůta splatnosti faktury v délce 30 dnů.

6. Prodávající a kupující se dohodli, že kupující je oprávněn započíst své pohledávky vzniklé na základě této smlouvy oproti pohledávce prodávajícího na zaplacení celkové kupní ceny.

7. V případě, že k datu uskutečnění zdanitelného plnění dojde u prodávajícího k naplnění podmínek tzv. nespolehlivého plátce nebo prodávající ve faktuře uvede jako bankovní spojení pro úhradu kupní ceny jiný účet, než je účet zdanitelného plnění, který je správcem daně pro prodávajícího zveřejněn způsobem umožňujícím dálkový přístup, je kupující oprávněn uhradit část finančního závazku na uhrazení kupní ceny prodávajícímu ve výši vypočtené DPH přímo na účet příslušného správce daně. Postupem dle tohoto odstavce se finanční závazek kupujícího vůči prodávajícímu ve výši daně z přidané hodnoty odvedené kupujícím považuje za zcela uspokojený.

8. Kupující neposkytuje zálohy.

9. Platby budou probíhat výhradně v CZK.

IV.
Místo a doba plnění, dodací podmínky

1. Místem plnění je Náměstí Jana Palacha 2, 116 38.

2. Systém uvedený v čl. II této smlouvy prodávající kupujícímu dodá, nainstaluje, uvede do provozu, vyzkouší jeho plnou funkčnost, zaškolí obsluhu kupujícího v souladu s čl. II této smlouvy nejpozději do 4 kalendářních týdnů ode dne účinnosti této smlouvy. Za účelem splnění činnosti dle přechozí věty se prodávající zavazuje, že bude zástupce prodávajícího přítomen v místě plnění po dobu instalace systému.

3. O přesném termínu dodání systému bude prodávající kupujícího informovat a to nejpozději 5 pracovních dnů před realizací dodávky.

4. Závazek prodávajícího dodat systém se považuje dle této smlouvy za splněný, pokud systém byl:
   a) řádně a včas předáno kupujícímu, vč. příslušné dokumentace
   b) řádně a včas instalováno, uvedeno do provozu a vyzkoušena jeho plná funkčnost
   c) řádně a včas zaškolena obsluha (3 uživatelé-zaměstnanci kupujícího)
   d) řádně a včas protokolárně převzato kupujícím.

5. Po splnění dodávky systému bude vyhotoven předávací protokol o předání a převzetí předmětu plnění, který bude obsahovat:
   a) název a sídlo prodávajícího a kupujícího
   b) označení kupní smlouvy
   c) označení dodaného předmětu plnění
   d) datum dodání, instalace a zaškolení obsluhy kupujícího
   e) stav předmětu plnění v době předání a převzetí
   f) seznam předaných dokladů
   g) seznam zaškolených osob
   h) podpisy oprávněných zástupců smluvních stran.

6. Zjevné vady při dodání systému je kupující povinen vytknout prodávajícímu při převzetí systému, skryté vady je kupující povinen sdělit prodávajícímu bez zbytečného odkladu poté, co je zjistí.

7. Kupující není povinen systém převzít, bude-li jevit jakékoliv znaky poškození či jiné zjevné vady. O odmítnutí převzetí systému bude sepsán záznam.

8. V případě, že budou při předání systému zjištěny drobné vady nebránící užívání systému, uvedou se do Přejímacího protokolu, včetně dohodnutého termínu jejich odstranění.

9. Za kupujícího je systém oprávněn převzít a Přejímací protokol podepsat:
   - kontaktní osoba : [redacted]
   - tel.č.: [redacted]
   - e-mail: [redacted]

V.
Právo užívání a nebezpečí škody systému

1. Kupující nabývá právo užívání k systému okamžikem úplného uhrazení kupní ceny.

2. Nebezpečí škody na systému přechází na kupujícího okamžikem protokolárního předání a převzetí systému od prodávajícího.

VI.
Odpovědnost za vady, záruka za jakost

1. Prodávající poskytuje záruku za jakost na každou dílčí část předmětu koupě v délce 60 měsíců ode dne následujícího po podpisu Přejímacího protokolu oběma smluvními stranami.

2. Záruční doba se prodlužuje o dobu trvání vady, která brání řádnému užívání systému. Doba od uplatnění práva z odpovědnosti za vady až do doby odstranění vady se nepočítá do záruční doby daného systému; po tuto dobu záruční doba neběží. V případě odstranění vady dodáním náhradního plnění běží pro toto náhradní plnění nová záruční doba v původní délce, a to ode dne jeho protokolárního převzetí kupujícím.

3. Zárukou za jakost se prodávající zavazuje, že systém bude po dobu běhu záruční doby způsobilý k použití pro sjednaný a obvyklý účel a že si zachová sjednané a obvyklé vlastnosti. V této souvislosti smluvní strany dohodly, že za sjednaný účel a sjednané vlastnosti považují účel a vlastnosti vyplývající z Přílohy č. 1 této smlouvy.

4. Zárukou za jakost nejsou dotčena ani omezena práva kupujícího z vadného plnění vyplývající z příslušných ustanovení občanského zákoníku, ať už se jedná o vady plnění, které jsou podstatným či nepodstatným porušením kupní smlouvy.

5. Prodávající se zavazuje po dobu trvání záruční doby poskytovat kupujícímu technickou podporu a záruční servis v souladu s podmínkami uvedenými v této smlouvě a jejich přílohách.

6. Vady, které se na systému projeví v záruční době, se zavazuje prodávající odstranit na vlastní náklady ve lhůtě do 1 pracovního dne od oznámení kupujícím, přičemž se prodávající zavazuje zahájit servisní zásah dle této smlouvy do 1 hod. od nahlášení závady kupujícím. Prodávající je povinen odstranit vady na své náklady tak, aby kupujícímu nevznikly žádné vícenáklady. Jestliže kupujícímu vícenáklady přesto vzniknou, hradí je prodávající. O odstranění vady bude sepsán protokol, který podepíší obě smluvní strany, návrh protokolu připraví prodávající.

   Oznamování záručních vad a potřeby záručního servisu bude kupující prodávajícímu oznamovat na těchto kontaktních spojeních:

   - kontaktní osoba: [redacted]
   - tel.č.:
   - e-mail:

7. V případě oznámení reklamace e-mailem se za den uplatnění reklamačního nároku (tj. nároku z poskytnuté záruky za jakost) považuje den prokazatelného odeslání e-mailu kupujícího na e-mailovou adresu prodávajícího uvedenou v odst. 2. tohoto článku.

8. Pokud prodávající nepřistoupí k vyřízení reklamačního nároku kupujícího podle této smlouvy, je kupující oprávněn k odstranění reklamované vady třetí odbornou osobou, přičemž náklady spojené s takovou opravou jdou plně k tíži prodávajícího a prodávající se zavazuje takové náklady kupujícímu uhradit na písemnou výzvu kupujícího doručenou do sídla prodávajícího.

VII.
Smluvní pokuta a úrok z prodlení

1. V případě, že bude kupující v prodlení s úhradou kupní ceny, je povinen zaplatit prodávajícímu za každý, byť i započatý kalendářní den prodlení s úhradou dle této smlouvy, smluvní pokutu ve výši 0,015 % z celkové kupní ceny.

2. Bude-li prodávající v prodlení s plněním dle této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu:
   a. za každý, byť i započatý kalendářní den prodlení se splněním dodávky dle této smlouvy, smluvní pokutu ve výši 0,2 % z celkové kupní ceny bez DPH
   b. za každý, byť i započatý den prodlení s odstraňováním vad oznámených kupujícím v záruční době ve stanovených lhůtách, smluvní pokutu ve výši 0,05 % z celkové kupní ceny bez DPH.

3. Smluvní strana, která poruší povinnosti vyplývající z této smlouvy, je povinna zaplatit druhé smluvní straně sjednanou smluvní pokutu ve výši dle tohoto článku za každé porušení její povinnosti, a to do 15 dnů ode dne doručení písemné výzvy strany oprávněné zaslané na adresu strany povinné, uvedenou v záhlaví této smlouvy, anebo

na její poslední známou adresu. Právo na náhradu vzniklé škody není zaplacením smluvní pokuty dle tohoto článku dotčeno.

4. Zaplacení smluvní pokuty nezbavuje povinnou stranu povinnosti splnit svůj závazek smluvní pokutou utvrzený. Kupující je oprávněn požadovat po prodávajícím rovněž náhradu škody vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje. Pro případ, že by byla smluvní pokuta soudem snížena, dohodly se zároveň smluvní strany, že zůstává zachováno právo na náhradu škody ve výši, v jaké škoda převyšuje částku určenou soudem jako přiměřenou. Smluvní pokuty dle této smlouvy lze kumulovat bez omezení.

VIII.
Doba trvání této smlouvy

1. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední smluvní stranou a uzavírá se na dobu určitou, a to do řádného splnění předmětu plnění. Zánikem (skončením) účinnosti této smlouvy zanikají všechny závazky smluvních stran z ní plynoucí s výjimkou nároků smluvních stran na náhradu újmy a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklých před skončením účinnosti smlouvy, a nezanikají rovněž závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví platný obecně závazný právní předpis.

2. Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy, přičemž za podstatné porušení této smlouvy se zejména považuje:
   a) na straně kupujícího nezaplacení kupní ceny podle této smlouvy ve lhůtě delší 30 dní po dni splatnosti příslušné faktury;
   b) na straně prodávajícího, jestliže nedodá řádně a včas předmět této smlouvy ve lhůtě delší 30 dní po smluvené době plnění.

3. Smluvní strana porušením povinnosti dotčená je povinna odstoupení od smlouvy písemně oznámit druhé smluvní straně na adresu uvedenou v záhlaví této smlouvy, anebo na její poslední známou adresu.

4. Odstoupením od smlouvy není dotčeno právo oprávněné strany na smluvní pokutu, ani právo oprávněné strany na náhradu škody.

IX.
Ostatní ujednání

1. Kupující se zavazuje umožnit přístup určeným pracovníkům prodávajícího do prostoru svého objektu za účelem splnění této smlouvy a provedení instalace předmětu plnění a dále pak za účelem následných oprav a servisních prací.

2. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními občanského zákoníku a dalšími platnými právními předpisy České republiky.

3. Ujednává se, že případné spory vzniklé z této smlouvy budou její účastníci řešit především vzájemnou dohodou, smírnou cestou. Pro řízení o případných sporných nárocích se ujednává příslušnost obecných soudů. Rozhodným právem je právo České republiky.

4. Kupující je oprávněn kontrolovat plnění předmětu této smlouvy prodávajícím.

5. Prodávající si je vědom, že ve smyslu ust. § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční

kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při finanční kontrole a že je povinen plnit další povinnosti v souvislosti s výkonem kontroly dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů. V tomto smyslu se dodavatel zavazuje poskytnout, v rámci kontroly dle předchozí věty, potřebnou součinnost v rozsahu daném uvedeným zákonem a poskytnout přístup ke všem dokumentům souvisejícím se zadáním a realizací předmětu této smlouvy, včetně dokumentů podléhajících ochraně podle zvláštních právních předpisů. K této povinnosti je prodávající povinen zavázat rovněž své poddodavatele v případě, že jejich prostřednictvím bude poskytovat část předmětu plnění této smlouvy. Prodávající je povinen zajistit a financovat veškerá případná poddodavatelská plnění nutná k řádnému splnění jeho povinností dle této smlouvy a nese za ně odpovědnost v plném rozsahu. Prodávající je rovněž povinen poskytnout všem orgánům oprávněným k provádění kontroly/auditu (poskytovatel dotace, příslušný Řídicí orgán operačního programu, Ministerstvo financí, orgány finanční správy, Nejvyšší kontrolní úřad, Evropská komise a Evropský účetní dvůr, případně další orgány oprávněné k výkonu kontroly) veškeré informace a doklady týkající se dodavatelských a poddodavatelských činností souvisejících s realizací projektu.

6. Prodávající je povinen archivovat originální vyhotovení této smlouvy včetně jejích dodatků, originály účetních dokladů, Přejímací protokol, záznamy o elektronických úkonech a dalších dokladů vztahujících se k realizaci předmětu této smlouvy po dobu 10 let od ukončení zadávacího řízení nebo od změny závazku z této smlouvy, min. však do lhůty 31. 12. 2033, po kterou musí být originální dokumenty k dispozici kontrolním orgánům, pokud legislativa nestanovuje pro některé typy dokumentů dobu delší (např. zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů). Lhůta byla nastavena s ohledem na čl. 140 obecného nařízení, které stanovuje, že doba, po kterou musí být originální dokumenty k dispozici Komisi a Evropskému účetnímu dvoru jsou dva roky od předložení účetní závěrky OP VVV, v níž jsou zahrnuty konečné výdaje ukončené činnosti a s ohledem na ustanovení § 44a odst. 11 rozpočtových pravidel (zákon č.218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla) ve znění pozdějších předpisů). Po tuto dobu je prodávající povinen umožnit osobám oprávněným k výkonu kontroly projektů provést kontrolu dokladů souvisejících s plněním této smlouvy, zejména poskytovat požadované informace a dokumentaci zaměstnancům nebo zmocněncům pověřených orgánů kontroly provádění projektu v rámci OP VVV, a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost. Dále musí být veškeré dokumenty a smluvní písemnosti zabezpečeny před ztrátou, odcizením nebo znehodnocením.

7. Uchovávání dokumentů a dokladů spisů spojených s OP VVV se řídí zákonem č. 499/2004 Sb., o archivnictví a spisové službě ve znění pozdějších předpisů, dále ustanoveními Obecného nařízení, zejména čl. 140, Nařízením Komise v přenesené pravomoci (EU) č. 480/2014, stanovující podrobné minimální požadavky na auditní stopu, pokud jde o účetní záznamy, které mají být uchovány, a o podklady, které mají být uchovávány na úrovni certifikačního orgánu, řídicího orgánu, zprostředkujících subjektů a příjemců podpory a Prováděcím nařízením Komise (EU) č. 821/2014 ze dne 28. července 2014, kterým se stanoví pravidla pro uplatňování nařízení (EU) č. 1303/2013 Evropského parlamentu a Rady, pokud jde o podrobná ujednání pro převod a správu příspěvků z programu, podávání zpráv o finančních nástrojích, technické vlastnosti informačních a komunikačních opatření k operacím a systém pro zaznamenávání a uchovávání údajů.

8. Prodávající je povinen být po celou dobu plnění dle této smlouvy pojištěn pojistnou smlouvou, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou prodávajícím třetí osobě v minimální výši 1 mil. Kč. Kupující je oprávněn kdykoliv

požádat prodávajícího o předložení pojistné smlouvy a prodávající je povinen tuto kupujícímu bez zbytečného odkladu předložit. Dojde-li na straně prodávajícího v průběhu plnění této smlouvy ke ztrátě pojištění odpovědnosti za škodu způsobenou prodávajícím třetí osobě, je prodávající povinen toto neprodleně obnovit. Porušení povinností prodávajícího dle tohoto odstavce se považuje za podstatné porušení smlouvy.

X.
Rozvazovací podmínka

Prodávající prohlašuje, že si je vědom skutečnosti, že kupující bude hradit kupní cenu dle článku III. této smlouvy z prostředků státního rozpočtu a Evropské unie na základě rozhodnutí MŠMT o poskytnutí dotace. V případě, kdy dotace MŠMT nebude poskytnuta do dne 30. 06. 2018, zanikají právní účinky této smlouvy dle ust. § 548 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a tato smlouva se tak od počátku zruší. Ke zrušení smlouvy z tohoto důvodu pak dojde jednostranným písemným oznámením kupujícího prodávajícímu na adresu jeho sídla, že dotace od MŠMT nebyla udělena a že se tato smlouva považuje za zrušenou bez dalšího, a to dnem doručení tohoto písemného oznámení. Pokud dojde mezi smluvními stranami v době platnosti a účinnosti smlouvy k nějakému vzájemnému plnění, jsou smluvní strany povinny si tato plnění bezodkladně vrátit. V případě, že výše uvedená dotace od MŠMT bude kupujícímu poskytnuta do termínu 30. 06. 2018, oznámí kupující tuto skutečnost prodávajícímu bezodkladně, smlouva zůstane v platnosti a účinnosti a smluvní strany začnou uskutečňovat svá další vzájemná plnění dle smlouvy.

XI.
Odkládací podmínka

Prodávající prohlašuje, že si je vědom skutečnosti, že kupující bude hradit kupní cenu dle článku III. této smlouvy z prostředků státního rozpočtu na základě rozhodnutí MŠMT o poskytnutí dotace. Tato smlouva dle ust. § 548 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, nabyde účinnosti dnem vydání uvedeného rozhodnutí MŠMT o poskytnutí dotace. O vydání rozhodnutí MŠMT bude kupující prodávajícího bezodkladně informovat.

XII.
Závěrečná ustanovení

1. Smluvní strany berou na vědomí, že kupující je subjektem podle § 2 odst. 1 písm. e) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, a na smlouvy jí uzavírané se vztahuje povinnost uveřejnění prostřednictvím registru smluv podle tohoto zákona (dále jen uveřejnění). Prodávající uděluje kupujícímu souhlas k uveřejnění této smlouvy včetně její přílohy i všech jejích dodatků v registru smluv, příp. i na profilu kupujícího jako zadavatele, a to včetně úkonů a okolností s touto smlouvou souvisejících. Smluvní strany se dohodly, že smlouva bude uveřejněna jako celek s vyloučením informací, které nelze poskytnout při postupu podle předpisů upravujících svobodný přístup k informacím z důvodu ochrany osobních údajů nebo bankovního tajemství. Uveřejnění smlouvy zajistí kupující neprodleně po uzavření smlouvy. Kupující se současně zavazuje informovat druhou smluvní stranu o provedení registrace tak, že zašle druhé smluvní straně kopii potvrzení správce registru smluv o uveřejnění smlouvy bez zbytečného odkladu poté, kdy sám potvrzení obdrží, popř. již v průvodním formuláři vyplní příslušnou kolonku s ID datové schránky prodávajícího (v takovém případě potvrzení od správce registru smluv o provedení registrace smlouvy obdrží obě smluvní strany současně).

2. Smlouvu lze měnit a doplňovat po vzájemné dohodě smluvních stran výhradně formou písemných vzestupně číslovaných dodatků, které obsahují dohodu stran o celém textu smlouvy a které jsou podepsány zástupci smluvních stran oprávněnými k takovým jednáním. Dodatky se po podpisu oběma smluvními stranami stávají nedílnou součástí této smlouvy. Ke změně smlouvy učiněné jinou než sjednanou formou se nepřihlíží. Za písemnou formu nebude pro tento účel považována výměna e-mailových, nebo jiných elektronických zpráv. V případě změny závazku ze smlouvy a ukončení závazku ze smlouvy bude kupující jako zadavatel postupovat dle §§ 222 a 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

3. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti okamžikem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., ve znění pozdějších předpisů, nebo dnem vydání rozhodnutí o poskytnutí dotace, pokud tato skutečnost nastane později. Pokud by se v důsledku změny právních předpisů nebo z jiných důvodů stala některá ujednání této smlouvy neplatnými nebo neúčinnými, budou tato ustanovení vyjasněna ve smyslu § 553 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů nebo po vzájemné dohodě nahrazena novým ustanovením, jež nejblíže, v rozsahu povoleném právními předpisy České republiky, odpovídá úmyslu smluvních stan v době uzavření této smlouvy. Smluvní strany prohlašují, že smlouva je ve zbývajících ustanoveních platná, neodporuje-li to jejímu účelu nebo nejedná-li se o ustanovení, která oddělit nelze v souladu s § 576 zákona č. 89/2012 Sb., občanský zákoník.

4. Ukáže-li se některé z ustanovení této smlouvy zdánlivým (nicotným), posoudí se vliv této vady na ostatní ustanovení smlouvy obdobně podle § 576 občanského zákoníku.

5. Smluvní strany výslovně sjednávají, že tato smlouva vyvolává právní následky, které jsou v ní samotné vyjádřeny, jakož i právní následky plynoucí ze zákona a dobrých mravů. Jiné právní následky smluvní strany vylučují.

6. Práva vzniklá z této smlouvy nesmí být postoupena bez předchozího písemného souhlasu druhé strany. Za písemnou formu nebude pro tento účel považována výměna e-mailových či jiných elektronických zpráv.

7. Tato smlouva obsahuje úplné ujednání o předmětu smlouvy a všech náležitostech, které strany měly a chtěly ve smlouvě ujednat, a které považují za důležité pro závaznost této smlouvy. Žádný projev stran učiněný při jednání o této smlouvě ani projev učiněný po uzavření této smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními této smlouvy a nezakládá žádný závazek žádné ze stran.

8. Strany si nepřejí, aby nad rámec výslovných ustanovení této smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.

9. Smluvní strany prohlašují, že si tuto smlouvu přečetly, s jejím obsahem souhlasí, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nápadně nevýhodných podmínek. Na důkaz toho připojují smluvní strany své podpisy.

10. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, přičemž kupující obdrží jedno vyhotovení a prodávající jedno vyhotovení.

11. Nedílnou součástí této smlouvy jsou její přílohy:
příloha č. 1 – Technická specifikace

V Praze dne 16. 8. 2018

[redacted]

doc. PhDr. Michal Pullmann, Ph.D., děkan

V Praze dne 15. 8. 2018

[redacted]

Ing. Jan Šíp, statutární ředitel
Networksys a.s.

[redacted]

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Technická specifikace – Aktivní síťové prvky

Technická specifikace pro následující zařízení:

- 2 ks Firewally pro počítačovou síť FF UK
- 13 ks Switche/Přepínače pro počítačovou síť FF UK
- 52 ks WiFi Access Pointy pro bezdrátovou síť FF UK
- 2 ks WiFi kontrolery pro bezdrátovou síť FF UK

Obecné podmínky

- Uchazeč je povinen v nabídce doložit skutečnost, že je partnerem výrobce pro prodej a servis nabízených aktivních prvků.
- Součástí veškerého nabízeného plnění budou i všechny potřebné licence (HW, SW), které budou již zahrnuty v nabídkové ceně.
- Součástí dodávky jsou rovněž konzultace zadavatele formou fyzické přítomnosti zástupce vybraného uchazeče na místě plnění veřejné zakázky.
- Součástí dodávky je doprava do místa plnění.
- Součástí dodávky je instalace a montáž zařízení v objektu FF UK, nám. J. Palacha 2, 116 38, Praha 1.
- Veškerý dodaný HW i SW musí být nový, nepoužitý a určený výrobcem pro český trh a Zadavatele, a musí být bez jakýchkoli právních vad. O této skutečnosti učiní uchazeč v nabídce čestné prohlášení. Uchazeč je povinen na vyžádání zadavatele předložit potvrzení zastoupení výrobce o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení) a SW (seznam licenčních klíčů) pro český trh a Zadavatele.
- Uchazeč je povinen v rámci dodávky zajistit podporu veškerého dodaného HW a SW, a to za následujících podmínek:
    - Uchazeč je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem HW a SW tak, aby:
        - v případě závady na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné eskalovat závadu přímo k výrobci zařízení,
        - zajistil Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje,
        - poskytnul Zadavateli po dobu trvání podpory všechny relevantní SW releases a verze SW nabízené výrobcem pro veškeré nabízené plnění. Uchazeč se zároveň zavazuje informovat Zadavatele o nových SW verzích a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Uchazeč se dále zavazuje získat potřebný SW legálním způsobem za podmínek stanovených výrobcem zařízení.
        - Součástí dodávky je instalace HW v místě dodání (demontáž původního HW, montáž nového a přenesení konfigurace z původního zařízení se zachováním stávajících funkcionalit). Součástí dodávky není instalace bezdrátových přístupových bodů.
    - Uchazeč je povinen na vyžádání zadavatele předložit potvrzení zastoupení výrobce veškerého dodaného HW a SW o řádně uzavřené dohodě o podpoře ve výše uvedeném rozsahu.

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Uchazeč v rámci nabídky dokládá skutečnost, že je certifikovaným partnerem výrobce pro prodej a servis nabízených zařízení v České republice na nejvyšší možné certifikované úrovni.

Technická specifikace: Firewally pro počítačovou síť FF UK

Základní popis

Zařízení určené k ochraně síťového prostředí před hrozbami na bázi pokročilých útoků. Kromě funkcí tzv. Nex.Gen FW (typicky chápané jako aplikační a identity-based FW) je schopno provádět inspekci provozu s detekcí a ochranou před útoky na úrovni síťového provozu. V oblasti ochrany proti malware je možnos aktivovat analýzu souborů včetně dynamické analýzy (tzv. sandboxing) i ukládání nebezpečných souborů do karantény. Zařízení lze použít i pro URL filtraci na úrovni kategorií, konkrétních URL či podle reputace serverů v Internetu. Integrované „Security Intelligence" database poskytují informace o nebezpečných IP adresách, URL, DNS doménách v Internetu. Centralizovaný management disponuje funkcemi korelace a automatizace: filtrace důležitých událostí, automatické nastavení detekčních jednotek podle typu provozu v síti, zohlednění útoků podle jejich nebezpečnosti v konkrétním prostředí, interakce s externími systémy v případě detekování nebezpečné aktivity v síti. V oblasti řízení přístupu podle informace o koncovém zařízení (tzv. kontext podává mnohem bohatší informaci o uživateli, koncovém zařízení, místě, metodě přístupu, apod.) je možná interakce s externími systémy řídící přístup do sítě podle kontextu. Kromě bezpečnostních funkcí poskytuje centralizovaný management pohled na kompletní síťovou aktivitu: směr komunikace na úrovni států, objemy datového přenostu podle URL, uživatele, aplikace, typu soborů, apod., viditelnost až do úrovně typů operačních systémů v síti. Toto je možné díky hloubkové analýze provozu, čímž máme k dispozici mnohem bohatší informace než poskytují běžné network monitoring systémy např na principu netflow. Interní korelační nástroje automaticky vyhodnocují stanice které mohly být kompromitovány či jsou vzdáleně ovládány. V neposlední řadě je k dispozici flexibilní reporting i možnost napojení prakticky na libovolný SIEM. Pro specifické aplikace může být využito API pro přístup k informacím a interním databázím centrálního managementu.

Tabulka parametrů

Dodané zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Uchazeč dle nabízeného zařízení**
Výkon a funkcionalita firewallu		
Formát zařízení	Appliance, 1RU	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management	1	1
Minimální počet 1Gb 10/100/1000 BaseT datových Ethernet rozhraní, standardně osazených	12	12
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	4	4
Možnost rozšíření o moduly rozhraní	1	1

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Možnost rozšíření o další 10Gb SFP+ rozhraní	8	8
Redundantní zdroje	Ano	ANO
Podporovaný počet současně otevřených spojení aplikačního FW	3M	3M
Rychlost vytváření nových spojení aplikačního FW	40K/s	40K/s
Propustnost aplikačního FW (top parametry)	8.5 Gbps	8.5 Gbps
Propustnost aplikačního FW + IPS (top parametry)	8.5 Gbps	8.5 Gbps
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	1024
Podpora stateful failover	active/standby	active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano	Ano
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	Ano	Ano
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	Ano	Ano
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	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
Podpora NAT64 a DNS64	Ano	Ano

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

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
Možnost řízení rychlosti datových toků na úrovni pravidel FW	Ano	Ano
Možnost rozšíření o funkce IPS	Ano	Ano
Možnost rozšíření o funkce URL filtrace	Ano	Ano
Možnost rozšíření o funkce antimalware filtrace	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
Funkce IPS a anti-malware		
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 obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	Ano
Podpora 802.1Q tagovaných rámců	Ano	Ano
Podpora různých IPS politik pro různé typy provozu	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
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano	Ano
Podpora vrstvev 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 doddavatele 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 možné nasadit plně transparentně 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
Funkce Next-Gen FW		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	Ano
Podpora pasivního monitorování (TAP režim)	Ano	Ano
Podpora 802.1Q tagovaných rámců	Ano	Ano
Počet podporovaných aplikací	Min. 3000	3000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	Ano
URL kategorií	80	80
Katagorizovaných světových URL	280 milionů	280 milionů
Řízení 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 Inteligence database – známé uzly botnet sítí C&C	Ano	Ano
Security Inteligence database – známé adresy anonymních proxy,	Ano	Ano

otevřených mail relay, apod.		
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	Ano	Ano
Možnost integrovat vlastní reputační database	Ano	Ano
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	Ano
Filtry mohou zohlednit roli a identitu uživatele	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	Ano	Ano
Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní

	Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact" aplikace Množství přenesených dat	Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact" aplikace Množství přenesených dat
Správa		
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	Ano
Přístup ke GUI http/https protokolem	Ano	Ano
Možnost vzdáleného přístupem protokolem ssh přímo do FW	Ano	Ano
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	Ano
Možnost centrální správy při nasazení více firewallů	Ano	Ano
Při centrální správě: možnost sdílených bezpečnostních politik	Ano	Ano
Při použití clusteru se spravuje pouze jeden logický prvek	Ano	Ano
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	Ano
Zobrazení logů a událostí v grafickém rozhraní správy	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 RADIUS server.	Ano	Ano
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	Ano
Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat,	Ano	Ano

korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)		
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 BMC Remedy Trustwave	ArcSight BMC Remedy Trustwave

	NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk	NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	Ano
Podpora 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
Zákaznicky 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
Záruka	60 měsíců / NBD	60 měsíců / NBD

Technická specifikace: Switche/Přepínače pro počítačovou síť FF UK

Základní popis

Síťové přepínače (switche), které jsou stohovatelné a nabízející enterprise funkce, rozšiřitelnost, bezpečnostní funkce a nízkou spotřebu energie.

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Součástí dodávky je software pro centralizovaný management síťových prvků a včetně licencí pro už existující zařízení v síti FF UK. Software musí podporovat ostatní aktivní síťové prvky, které jsou součástí nabídky a obsahovat všechny potřebné licence.

Tabulka parametrů přepínače

Dodané zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality / vlastnosti**	**Doplní Uchazeč dle nabízeného zařízení**
Základní vlastnosti		
Počet PoE portů 10/100/1000	48	48
Počet portů 10 Gbit/s a jejich typ	2x SFP+	2x SFP+
Výkonnostní parametry		
Minimální paketový výkon přepínače v paketech/vteřinu	130 milionu	130,9 milionu
PoE		
PoE výkon k dispozici	370W	370W
počet najednou fungujících PoE (IEEE 802.3af) portů	24	24
počet najednou fungujících PoE+ (IEEE 802.3at) portů	12	12
Třída a formát zařízení		
Třída zařízení	L2 switch	L2/L3
Formát zařízení	1RU	1RU
Minimální propustnost přepínacího subsystému	200 Gbit/s	200 Gbit/s
Minimální počet MAC adres	15000	16000
Možnost připojit externí redundantní zdroj	ano	ano
Vlastnosti stohování		
Stohovatelný	ano	ano
Stohovatelný bez snížení počtu ethernet portů	ano, volitelným modulem	ano, volitelným modulem
Rychlost stohovacího propojení	alespoň 80 Gbit/s	80 Gbit/s
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	8
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 řídícím prvkem stohu (1:N redundance)	ano	ano
QoS na stohovacím propoji	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	1023
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	8 per port
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
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
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		
OSPFv2, OSPFv3	ano	ano
RIPv2	ano	ano
statické směrování	ano	ano
Policy-based routing podle ACL	ano	ano
Směrování multicastu		
PIM	ano	ano
IGMPv2 snooping	ano	ano
IGMPv3 snooping	ano	ano
IPv6 MLDv1 & v2 snooping	ano	ano

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Bezpečnost		
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
konfiguorvatelná 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-05 nebo funkčně ekvivalentní).	ano	ano
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ano	ano
Podpora kontroly autenticity operačního systému switche, podpora kontroly integrity operačního systému switche při bootování kontrolou digitálního podpisu. Nutné pro ověření, že operační systém switche nikdo před či při bootování nikdo nemodifikoval.	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		
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		
CLI rozhraní	ano	ano
SSHv2	ano	ano
SSHv2 over IPv6	ano	ano

Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ano
SNMPv2 a v3	ano	ano
USB a 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
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
Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí nástroje pro centrální správu - management (viz tabulka dále).	ano	ano
Služby		
DHCP server	ano	ano
Záruka	60 měsíců / NBD	60 měsíců / NBD

Tabulka parametrů software pro centralizovaný management síťových prvků

Dodaný software musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované**	**Doplní Uchazeč dle nabízeného**

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

	funkcionality /vlastnosti	**zařízení**
Licence pro připravený virtuální obraz do virtualizovaného prostředí	ano	ano
Podpora Windows 2016 server	ano	ano
Maximální nároky na virtuální prostředí	4vCPU, 14 GB RAM, 350 GB Disk, 200MBps I/O	4vCPU, 14 GB RAM, 350 GB Disk, 200MBps I/O
Podporovaných síťových zařízení celkem	400	500
Podporovaných síťových zařízení - aktivních prvků (přepínače, směrovače)	250	300
Podporovaných systémů pro víceúrovňový vhled a analýzu síťového provozu	4	5
Podporovaných fyzicky připojených klientů k aktivním prvkům	5500	6000
Událostí zpracovaných za jednu sekundu celkem	100	100
Syslog zpráv zpracovaných za jednu sekundu	50	70
SNMP trapů zpracovaných za jednu sekundu	20	20
Systémových událostí zpracovaných za jednu sekundu	10	10
Zpracovaných toků Netflow - Netflow flow za sekundu	2500	3000
Monitorovaných síťových rozhraní (polling)	2000	2400
Platforma		
Bezpečný přístup prostřednictvím webového grafického uživatelského rozhraní	Ano	Ano
Podpora autorizace a autentizace přístupu do systému vůči TACACS+	Ano	Ano
Podpora autorizace a autentizace přístupu do systému vůči RADIUS	Ano	Ano
Podpora řízení přístupu ke GUI pomocí identity (SSO - Single Sign On)	Ano	Ano
Podpora různých úrovní oprávnění pro přístup do systému (RBAC)	Ano	Ano
Podpora multiuživatelského prostředí GUI s možností využít jak předdefinované skupiny, tak s možností definovat vlastní přístupová oprávnění k funkcím GUI pro alespoň dvě uživatelské skupiny	Ano	Ano
Podpora přístupu ke GUI z mobilních zařízení, např. tabletů	Ano	Ano
Podpora logování aktivity uživatelů a logování systémových událostí	Ano	Ano
Podpora zálohování systému a obnovy ze zálohy	Ano	Ano
Možnost změnit nastavení doby ukládání historických a agregovaných dat	Ano	Ano
Možnost omezit přístup uživatelům pouze ke skupině zařízení, např. na základě lokality, typů zařízení apod.	Ano	Ano
Možnost monitoringu provozních parametrů aplikací	Ano	Ano
Možnost zpracování informací o provozu v sítí (NetFlow) včetně deduplikace dat z více zdrojů	Ano	Ano

Možnost zobrazit informace o chování aplikací v síti (statistiky, identifikace případných problémů na síťové nebo aplikační úrovni, zhoršení uživatelské zkušenosti uživatelů)	Ano	Ano
Podpora protokolu IPv4	Ano	Ano
Podpora protokolu IPv6	Ano	Ano
Podpora protokolu SSH	Ano	Ano
Podpora protokolů SNMPv1, SNMPv2, SNMPv2c a SNMPv3	Ano	Ano
Podpora zpracování SYSLOG zpráv	Ano	Ano
Podpora zpracování SNMP zpráv	Ano	Ano
Možnost úpravy zpracování událostí a alarmů včetně např. potlačení vybraných alarmů	Ano	Ano
Možnost kategorizace alarmů a událostí	Ano	Ano
Možnost nastavit zasílání upozornění na vybrané události emailem	Ano	Ano
Podpora MIB třetích stran	Ano	Ano
Možnost monitoringu parametrů definovaných v MIB třetích stran	Ano	Ano
Možnost definovat vlastní události na základě SNMP nebo SYSLOG zpráv	Ano	Ano
Možnost exportu zpráva a událostí	Ano	Ano
Možnost generovat zprávy pro nadřazený management systém	Ano	Ano
Posílání alarmů a událostí network management aplikacím třetích stran, které podporují FCAPS	Ano	Ano
Podpora API pro programatický přístup k funkcionalitě aplikace správy	Ano	Ano
Schopnost management systému nalézt automaticky zařízení v síti s využitím více různých metod pracujících s informacemi z druhé a třetí vrstvy	Ano	Ano
Schopnost management systému filtrovat nalezená zařízení – vyloučit resp zahrnout definované adresní rozsahy	Ano	Ano
Schopnost management systému připravit konfigurační a jiné změny formou úlohy včetně schvalovacích mechanizmů	Ano	Ano
Podpora pro vyhledávání informací o síťových zařízení, připojených koncových zařízení, uživatelích, konfigurovaných parametrech, alaremech, událostech apod. napříč celým management systémem.	Ano	Ano
Správa aktivních prvků		
Požadavky na škálování - systém musí být schopen kromě LAN / WAN sítě spravovat a monitorovat také bezdrátovou síť pouhým přidáním příslušných licencí	Ano	Ano
Kompletní správa životního cyklu LAN / WAN sítě (plánování, nasazení, monitoring, troubleshooting, reporting)	Ano	Ano
Inventarizace HW síťových prvků	Ano	Ano
Inventarizace, nasazení a správa firmware aktivních prvků	Ano	Ano
Analýza vhodnosti firmware aktivních prvků pro nasazení	Ano	Ano
Generování reportů inventory aktivních prvků	Ano	Ano
Konfigurace pomocí šablon pro zefektivnění konfiguračních úloh	Ano	Ano
Inventarizace, verzování, archivace a správa konfigurací LAN/WAN sítě	Ano	Ano

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Předpřipravené šablony dle doporučení výrobce - "best practice"	Ano	Ano
Možnost udržovat konfigurace v souladu s firmním standardem, identifikovat neshody	Ano	Ano
Celkové konfigurační šablony sestavovány z dílčích šablon konfigurací jednotlivých funkcí nebo uživatelsky definovaných konfigurací jednotlivých funkcí	Ano	Ano
Podpora pro o automatizovanou konfiguraci nově připojovaných zařízení	Ano	Ano
Zobrazování alarmů a událostí z LAN / WAN sítě	Ano	Ano
Topologická mapa	Ano	Ano
Nástroje pro detekci a řešení problémů v LAN / WAN síti	Ano	Ano
Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení a jednotlivého uživatele v souhrnném pohledu (kontextově) pro rychlejší troubleshootnig	Ano	Ano
Zobrazení informací o uživateli, koncovém či síťovém zařízení v kontextu informací souvisejících s jeho okolím a provozními parametry	Ano	Ano
Detailní monitoring LAN / WAN sítě	Ano	Ano
Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí	Ano	Ano
Monitorování výskytu koncových zařízení a uživatelů v síti	Ano	Ano
Monitoring a vyhodnocování přenosových parametrů z NetFlow	Ano	Ano
Monitoring funkčnosti (včetně odezev) přenášených aplikací	Ano	Ano
Monitoring parametrů zdraví aktivních prvků a jejich přehledné zobrazení	Ano	Ano
Možnost nastavit prahové hodnoty pro monitoring parametrů zdraví aktivních prvků	Ano	Ano
Monitoring IPv6 připojení koncových zařízení napříč pevnou i bezdrátovou sítí	Ano	Ano
Automatické dohledání portu pevné sítě s připojeným falešným access pointem	Ano	Ano
Možnost identifikovaný problém eskalovat prostředky management systému na podporu výrobce	Ano	Ano
Možnost integrace s další aplikací pro zjišťování identity, typu, parametrů, stavu a stavu software koncových klientů pevné i bezdrátové sítě; pro monitoring bezpečnostních politik koncových klientů	Ano	Ano
Uchazeč je povinen při dodávce zboží řádným způsobem uzavřít dohodu o podpoře s výrobcem managementu tak, aby v případě závady na dodaném software, kterou není Uchazeč schopen sám odstranit, bylo možné minimálně po dobu 2let tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost si sám legálně stahovat nové verze software přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního kontraktu.	Ano	Ano

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Technická specifikace: WiFi Access Pointy pro bezdrátovou síť FF UK

Základní popis

WiFi Access Pointy pro bezdrátovou síť, které jsou kompatibilní s kontrolery, které jsou součástí této nabídky, a centrálně spravovatelé pomocí software pro centralizovaný management síťových prvků, který je součástí této nabídky.

Tabulka parametrů WiFi Access Pointy

Dodané zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Uchazeč dle nabízeného zařízení**
Součástí dodávky je licence pro připojení k wifi AP kontrolerům, které jsou součástí této nabídky.	Ano	Ano
AP je podporován softwarem pro centralizovaný management síťových prvků, který je součástí této nabídky.	Ano	Ano
Typ antén	Integrované pro obě pásma	Integrované pro obě pásma
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, možnost provozovat jedno z rádií v monitorovacím režimu pro 2,4 i 5 GHz současně	ano	ano
Podpora standardů 802.11a/b/g/n a 802.11ac wave 2	ano	ano
Podpora 4x4 MIMO, podpora MU-MIMO, až 160 MHz kanál pro 802.11ac	ano	ano
Minimální počet inzerovaných SSID (BSSID) per radio	8	8
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 a/g/n/ac klientům (Beam Forming)	ano	ano
Podpora mechanismů pro přepojení klientů z 2,4GHz do 5GHz pásma a optimalizovaného roamingu	ano	ano
Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI	ano	ano
Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ano	ano
AP uzavřené konstrukce, bez větracích otvorů a ventilátoru	ano	ano

Access Pointy jsou fyzicky zabezpečitelné/zamknutelné k okolním pevným částem	ano	ano
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a pomocí Telnet a SSH	ano	ano
Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference)	ano	ano
Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur	ano	ano
2 x 10/100/1000 Ethernet rozhraní	ano	ano
Napájení AP pomocí 802.3at PoE	ano	ano
Součástí dodávky AP je i licence potřebná pro jeho registraci ke stávajícímu kontroleru Zadavatele a to vč. servisní podpory	ano	ano
Součástí každého AP musí být licence pro jeho centrální správu a monitoring pomocí software pro centralizovaný management síťových prvků, který je součástí této nabídky. Tento nástroj musí být plně podporován výrobcem zařízení a zařízení musí být na jeho seznamu 100% kompatibilních zařízení. Celkem se požaduje 60 licencí (52+8 rezerva)	ano	ano
Uchazeč povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.	ano	ano
Záruka	60 měsíců / NBD	60 měsíců / NBD

Technická specifikace: WiFi kontrolery pro bezdrátovou síť FF UK

Základní popis

WiFi kontrolery pro bezdrátovou síť v redundantní konfiguraci, které jsou kompatibilní s WiFi Access Pointy, které jsou součástí této nabídky, a centrálně spravovatelé pomocí software pro centralizovaný management síťových prvků, který je součástí této nabídky.

Tabulka parametrů WiFi kontrolery

Dodané zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Uchazeč dle nabízeného zařízení**
Kontroler bezdrátové sítě + redundantní zařízení	1+1 (dvojice v HA)	1+1 (dvojice v HA)
Minimální počet 10G SFP+ portů per kontroler	2	2

Příloha ZD č. 2i – Technická specifikace pro část I) Firewally pro počítačovou síť, Switche/Přepínače pro počítačovou síť, WiFi Access Pointy pro bezdrátovou síť, WiFi kontrolery pro bezdrátovou síť FF UK

Redundantní napájecí zdroj součástí dodávky	ano	ano
Minimální propustnost pro data Gb/s	20 Gb/s	20 Gb/s
Podpora až 1500 registrovaných AP při výpadku primárního kontroleru	ano	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
Lokální síť - možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost	ano	ano
Mesh síť - podpora indoor a outdoor mesh sítí, současné připojení normálních a mesh AP k jednomu kontroleru	ano	ano
Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP	ano	ano
Šifrovaná řídící komunikace AP-kontroler	ano	ano
Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů	ano	ano
Bezpečnost a Guest Access		
Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování	ano	ano
802.1x/EAP autentizace: PEAP, EAP-FAST, EAP-TLS, ...	ano	ano
Možnost autentizace nových klientů k AP v módu lokálního bridgování dat pomocí 802.1x/EAP i v případě výpadku centrálního kontroleru	ano	ano
Podpora standardu „802.11w“ pro ochranu řídících rámců na AP a klientovi	ano	ano
Podpora standardu „802.11u“ pro výběr SSID a autentizaci klienta	ano	ano
Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP	ano	ano
Integrovaná správa návštěvnických účtů s možností definice jejich platnosti	ano	ano
Možnost omezit počet klientů per SSID	ano	ano
Lokální profilování zařízení – per uživatel a per zařízení	ano	ano

Integrovaný IDS systém pro detekci útoků na bezdrátovou síť (wireless IDS), detekce cizích AP (Rogue AP) a klientů v AdHoc režimu, 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		
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 (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient, možnost nastavit konkrétní QoS profil na Apple klientech přímo z kontroleru	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
Podpora Apple Bojour protokolu, zpracování mDNS paketů, možnost filtrování služeb mezi subnety	ano	ano
Správa frekvenčního pásma		
Automatizovaná centrální správa frekvenčního pásma, spolupráce mezi kontrolery v clusteru	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), grafické vyobrazení informací o kvalitě signálu	ano	ano

Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing")	ano	ano
Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ano	ano
Mesh síť – automatický výběr vhodného kanálu pro backhaul, automatické sestavení optimálního mesh stromu, monitorování všech kanálů na pozadí s rychlou konvergencí v případě výpadku primárního nadřazeného AP	ano	ano
Troubleshooting radiového signálu a automatické řešení problému rušivého signálu, generování alarmů na základě překročení prahových hodnot kvality signálu	ano	ano
Možnost členění AP do skupin, konfigurace AP podle příslušnosti do skupiny	ano	ano
Možnost vytváření rádiových profilů (nastavení kanálů, rychlostí)	ano	ano
Nastavení různého rádiového profilu pro různé skupiny AP	ano	ano
Podpora IPv6		
Podpora IPv6 – management kontroleru (vč. Syslog, radius)	ano	ano
Podpora IPv6 – komunikace AP-kontroler	ano	ano
Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty	ano	ano
Podpora IPv6 – IPv6 multicast, MLD snooping	ano	ano
Podpora IPv6 – bezpečnost (RAGuard, IPv6 Source Guard, DHCPv6 Server Guard, ACL)	ano	ano
Podpora IPv6 – video-streaming se spolehlivým multicastem	ano	ano
Podpora IPv6 – ND cache na kontroleru, optimalizace přenosu ND zpráv, rate-limiting pro RA	ano	ano
Dohled a správa kontroleru		
Centrální administrace správců s granularitou přístupových práv	ano	ano
Podpora správy přes serial CLI nebo přes IPv4 a IPv6 pomocí SSH/telnet, http a https web GUI, SNMP, aplikace pro dohled pro Android a Apple mobilní platformy	ano	ano
RJ45 konzolový port a/nebo USB konzolový port	ano	ano
Záruka	60 měsíců NBD	60 měsíců NBD