Univerzita Pardubice

KUPNÍ SMLOUVA Č. 1309/19

Níže uvedeného dne, měsíce a roku smluvní strany:

Univerzita Pardubice
Právní forma: veřejná vysoká škola zřízená zákonem
Se sídlem: Studentská 95, 532 10 Pardubice
Zastoupená: prof. Ing. Jiřím Málkem, DrSc., rektorem
IČO: 00216275
DIČ: CZ00216275
Bankovní spojení: Komerční banka, a. s., pobočka Pardubice
Číslo účtu: [redacted]
Kontaktní osoba: [redacted]

(dále jen „kupující“)

a

ICT Energo, s.r.o.
Se sídlem/Místem podnikání: Palackého třída 441/91, 612 00 Brno
Zapsaná: v obchodním rejstříku vedeném Krajským soudem v Brně oddíl C, vložka 69668
Zastoupená: [redacted], jednatelem
IČO: 29268826
DIČ: CZ29268826
Bankovní spojení: Česká spořitelna, a.s.
Číslo účtu: [redacted]
Kontaktní osoba: [redacted]

(dále jen „prodávající”)

uzavřely dle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „OZ“) za účelem dodávky komponent bezpečnostní infrastruktury v rámci projektu OP VVV „Investiční podpora vzdělávacích aktivit na UPa“, reg. č. CZ.02.2.67/0.0/0.0/18_057/0013255 tuto kupní smlouvu (dále jen „smlouva“).

I. Předmět smlouvy

1. Prodávající se zavazuje, na základě své nabídky ze dne 17. 2. 2020 k veřejné zakázce s názvem **„Dodávka bezpečnostní infrastruktury“** (dále jen „Veřejná zakázka“), zadávané v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „ZZVZ“), dodat kupujícímu v rozsahu a za podmínek stanovených touto smlouvou bezpečnostní infrastrukturu včetně nezbytné dokumentace (dále jen „zboží“) a převést na kupujícího

vlastnické právo k tomuto zboží. Zboží je podrobně specifikováno v příloze č. 1 této smlouvy – „Technická specifikace".

2. Zboží musí být nové, nepoužité, plně funkční, nerenovované, kompletní a v souladu se specifikací uvedenou v příloze č. 1 této smlouvy a v souladu s přílohou č. 3 této smlouvy „Závazně používané standardy" tak, aby bylo možné jeho plné využití.

3. Prodávající je povinen zboží dodat do místa plnění dle čl. III. odst. 1. této smlouvy ve sjednaném množství, jakosti, provedení a čase.

4. Prodávající je povinen instalovat a uvést zboží do provozu včetně prověření a předvedení bezchybné funkčnosti zboží v místě a době plnění dle čl. III. této smlouvy.

5. Prodávající je povinen při předání zboží dle čl. IV. této smlouvy předat kupujícímu prohlášení o záruce (nebo jiné dokumenty potvrzující poskytnutí záruky výrobcem ve prospěch objednatele), resp. záruční list na zboží, technickou dokumentaci, uživatelské příručky a veškerou další dokumentaci potřebnou k provozování zboží v českém nebo anglickém jazyce.

6. Kupující se zavazuje zboží převzít a zaplatit prodávajícímu dohodnutou kupní cenu dle čl. II. odst. 1. této smlouvy.

II. Kupní cena

1. Smluvní strany se ve smyslu zákona č. 526/1990 Sb., o cenách, v platném znění, dohodly na této celkové kupní ceně zboží:

   Celková kupní cena zboží: 7 039 994,- Kč bez DPH

2. Sjednaná cena ve smlouvě je uvedena bez daně z přidané hodnoty a daň z přidané hodnoty bude k této ceně účtována dle daňových předpisů platných v okamžiku uskutečnění zdanitelného plnění, při vystavení daňového dokladu - faktury dle zákona č.235/2004 Sb. (dále jen „faktura").

3. Celková cena uvedená v odst. 1. tohoto článku a jednotkové ceny zboží uvedené v příloze č. 2 této smlouvy – „Výkaz výměr (položkový rozpočet)" jsou cenami nejvýše přípustnými a neměnnými po celou dobu účinnosti této. Ve sjednaných cenách jsou zahrnuty veškeré náklady prodávajícího spojené s plněním povinností dle této smlouvy (např. náklady na balné, skladné, dopravu, instalaci, pojištění, aj.). Prodávající není oprávněn účtovat žádné další částky v souvislosti s plněním dle této smlouvy.

III. Místo a doba plnění

1. Místem plnění je objekt Univerzity Pardubice, budova EA, na adrese: Studentská 84, 532 10 Pardubice. Osobou, kterou kupující pověřil k převzetí zboží, je kontaktní osoba uvedená v úvodních ustanoveních této smlouvy (dále jen „příjemce"), popř. jiná, kupujícím pověřená, osoba.

2. Prodávající je povinen řádně dodat kupujícímu zboží do místa plnění v rozsahu dle čl. I. této smlouvy nejpozději do 8 týdnů ode dne podpisu této smlouvy poslední smluvní stranou.

3. Prodávající je povinen dodat kupujícímu zboží v místě plnění v pracovních dnech od 08:00 hod. do 15:00 hod., mimo tuto dobu pouze ve výjimečných případech a po předchozí dohodě s příjemcem. Dále je povinen telefonicky vyrozumět příjemce o připravenosti dodat zboží, a to nejméně 3 pracovní dny předem.

IV. Předání a převzetí zboží

1. Povinnost prodávajícího dle čl. I. této smlouvy je považována za splněnou provedením přejímky zboží příjemcem či jeho pověřeným zástupcem a prodávajícím či jeho pověřeným zástupcem v místě a době plnění dle čl. III. této smlouvy. Kupující není povinen převzít zboží, které vykazuje jakoukoliv vadu či nedodělek.

2. Přejímkou se rozumí předání zboží včetně splnění všech podmínek stanovených v čl. I. této smlouvy prodávajícím a převzetí zboží příjemcem. Zjistí-li příjemce, že zboží trpí vadami, odmítne jeho převzetí s vytčením vad. O takovém odmítnutí sepíší smluvní strany zápis. Povinnost prodávajícího dle čl. III. odst. 2. této smlouvy tím není dotčena.

3. O provedení přejímky bude prodávajícím a příjemcem sepsán přejímací protokol s uvedením data provedení přejímky. Toto datum je dnem dodání zboží a je rozhodné pro splnění povinnosti prodávajícího dle čl. III. odst. 2. této smlouvy. V přejímacím protokolu prodávající zejména uvede označení smluvních stran, označení zboží, jeho množství, čitelné jméno a podpis, příjemce uvede též své čitelné jméno a podpis.

4. Svépomocný prodej dle § 2126 a násl. OZ se nepoužije.

V. Fakturační a platební podmínky

1. Právo fakturovat vzniká prodávajícímu dnem řádného dodání zboží v rozsahu dle čl. I. této smlouvy.

2. Prodávající je povinen po vzniku práva fakturovat vystavit a do 15 dnů doručit kupujícímu originál daňového dokladu (dále jen „faktura“) za řádně dodané zboží za dohodnutou smluvní cenu. Faktura bude mít náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění (dále jen „ZDPH“). Na faktuře bude uvedeno evidenční číslo této smlouvy zaznamenané v jejím názvu a číslo interní objednávky kupujícího, které kupující sdělí prodávajícímu při podpisu smlouvy. Dále bude na faktuře uvedeno, že se jedná o dodávku pro projekt OP VVV „Investiční podpora vzdělávacích aktivit na UPa“, reg. č. CZ.02.2.67/0.0/0.0/18_057/0013255.

3. Společně s fakturou je prodávající povinen předložit též přejímací protokol potvrzený příjemcem.

4. Faktura může mít listinnou nebo elektronickou podobu. Splatnost faktury činí 30 dnů – v případě listinné podoby ode dne jejího prokazatelného doručení na adresu sídla kupujícího uvedenou v úvodních ustanoveních této smlouvy, v případě elektronické podoby ode dne jejího prokazatelného doručení na e-mailovou adresu: fakturace@upce.cz. Odběratel tímto souhlasí

s elektronickou formou fakturace a zavazuje se neprodleně informovat dodavatele o jakékoliv změně e-mailové adresy pro zasílání faktur a dále se zavazuje, že zajistí řádnou funkčnost uvedené e-mailové adresy po dobu trvání této smlouvy. Jestliže bude z okolnosti zřejmé, že fakturu nelze na uvedenou e-mailovou adresu doručit, např. se zpráva vrátí jako nedoručitelná, bude neprodleně na adresu sídla kupujícího uvedenou v úvodních ustanoveních této smlouvy zaslána faktura v papírové podobě, přičemž však bude faktura splatná v termínu, jakoby byla úspěšně doručena prostřednictvím e-mailu..

5. V případě, že faktura bude obsahovat nesprávné nebo neúplné údaje nebo k ní nebudou přiloženy požadované doklady, je kupující oprávněn vrátit ji do data její splatnosti prodávajícímu, aniž se tak dostane do prodlení se splatností. Prodávající vrácenou fakturu opraví, eventuálně vyhotoví novou, bezvadnou. V takovém případě běží kupujícímu nová doba splatnosti dle odst. 4. tohoto článku ode dne doručení opravené nebo nové faktury.

6. Zaplacením kupní ceny se rozumí odepsání částky z účtu kupujícího a její směrování na účet prodávajícího.

7. Kupující neposkytuje zálohové platby. Platby budou probíhat výhradně v Kč. Celkovou cenu uhradí kupující formou bezhotovostního převodu na účet prodávajícího uvedený v úvodních ustanoveních této smlouvy.

8. Smluvní strany se dohodly, že nastane-li v souvislosti s prodávajícím jakákoliv skutečnost, v jejímž důsledku se může vůči kupujícímu uplatnit ručení za daň odváděnou prodávajícím ve smyslu ZDPH, je kupující oprávněn nezaplatit prodávajícímu vyúčtovanou DPH a odvést ji přímo správci daně a kupující je rovněž oprávněn odstoupit od této smlouvy.

9. Prodávající prohlašuje, že na sebe přebírá nebezpečí změny okolností podle § 1765 odst. 2 OZ, § 1765 odst. 1 a § 1766 OZ se tedy ve vztahu k prodávajícímu nepoužije.

VI. Práva a povinnosti smluvních stran, vlastnické právo a nebezpečí škody na zboží

1. Prodávající je povinen při plnění této smlouvy postupovat s odbornou péčí, dodržovat obecně závazné právní předpisy, normy a další předpisy vztahující se k předmětu smlouvy, podmínky této smlouvy a pokyny kupujícího.

2. Kupující se zavazuje poskytnout prodávajícímu při plnění předmětu této smlouvy nezbytnou součinnost.

3. Vlastnické právo ke zboží přechází z prodávajícího na kupujícího provedením přejímky zboží dle čl. IV. této smlouvy.

4. Nebezpečí škody na zboží přechází na kupujícího ve smyslu ustanovení § 2121 odst. 1 OZ provedením přejímky zboží dle čl. IV. této smlouvy.

Univerzita Pardubice

VII. Záruka za jakost, reklamační podmínky

1. Prodávající odpovídá za to, že zboží je ke dni dodání plně funkční a splňuje veškeré podmínky stanovené v této smlouvě a v příloze č. 1 této smlouvy – „Technická specifikace" a v příloze č. 3 této smlouvy – „Závazně používané standardy datových sítí". Prodávající prohlašuje, že předmět plnění nemá žádné právní vady, zejména není zatížen právy třetích osob.

2. Prodávající poskytuje kupujícímu záruku za jakost a vlastnosti dodaného zboží, jež odpovídá předmětu a účelu této smlouvy, v délce trvání 3 let. Pokud však výrobce zboží poskytuje záruku delší, platí i pro kupujícího tato delší záruční doba. Záruční doba počíná běžet dnem uvedeným v předávacím protokolu podepsaným oběma smluvními stranami (oprávněnými zástupci).

3. Kupující je povinen písemně (tj. i elektronicky) uplatnit zjištěné vady zboží (dále jen „reklamace"), bez zbytečného odkladu poté, co je zjistil. Prodávající je povinen kupujícímu doručit písemné (tj. i elektronicky) vyjádření k reklamaci ve smyslu § 2117 OZ s odkazem na § 2173 OZ v době 5 pracovních dnů po jejím obdržení. Pokud během této doby nebude kupujícímu doručeno písemné vyjádření prodávajícího k reklamované vadě, platí, že prodávající uznává reklamaci v plném rozsahu. I reklamace odeslaná kupujícím v poslední den záruční doby se považuje za včas uplatněnou.

4. Prodávající je povinen bezplatně odstranit reklamované vady, které uznal, nebo ke kterým se nevyjádřil podle odst. 3 tohoto článku, a to v místě plnění bez zbytečného odkladu, nejpozději však do 30 dní od doručení oznámení o reklamaci. Prodávající není oprávněn účtovat si v záruční době cestovní ani jiné obdobné náklady.

5. V případě prodlení prodávajícího s odstraněním vady v době uvedené v odst. 4 tohoto článku delší než 15 dnů je kupující oprávněn vadu na náklady prodávajícího odstranit sám nebo ji dát na náklady prodávajícího odstranit třetí osobou a prodávající je povinen tyto náklady uhradit nejpozději do 15 dnů ode dne doručení písemné výzvy kupujícího k tomuto zaplacení.

6. Prodávající je povinen reklamovanou vadu odstranit i tehdy, pokud se smluvní strany neshodnou na tom, že se jedná o oprávněnou reklamaci. Do doby vyřešení takovéhoto sporu jdou náklady spojené s odstraněním reklamované vady k tíži prodávajícího.

7. Způsob vyřízení reklamace určuje kupující. Kupující má právo uplatnit reklamaci i v případě, jedná-li se o vadu zboží, kterou musel s vynaložením obvyklé pozornosti poznat již při přejímce zboží.

8. Kromě povinnosti bezplatně odstranit reklamovanou vadu je prodávající povinen uhradit kupujícímu prokázanou škodu, která vznikla kupujícímu v souvislosti s vadným plněním prodávajícího.

9. Záruční doba se automaticky prodlužuje o počet dnů uplynulých od nahlášení vady do podpisu protokolu o odstranění vady.

10. Za vady, které se projevily po záruční době, odpovídá prodávající jen tehdy, pokud jejich příčinou bylo porušení jeho povinností.

11. Prodávající je dále povinen plnit další povinnosti související se zárukou uvedené v příslušných ustanoveních přílohy č. 1 této smlouvy - „Technická specifikace“.

12. Prodávající se v záruční době zavazuje bezplatně poskytovat informace servisním technikem prostřednictvím telefonického spojení a e-mailu, a to v pracovních dnech od 8:00 hod. do 16:00 hod. Telefonní číslo: [redacted], e-mail: [redacted].

VIII. Smluvní pokuty a úrok z prodlení

1. V případě prodlení prodávajícího s dodáním zboží (či jeho části) nebo se splněním povinnosti dle čl. I. této smlouvy ve sjednané době dle čl. III. odst. 2. této smlouvy, je kupující oprávněn požadovat po prodávajícím zaplacení smluvní pokuty ve výši 0,05 % z kupní ceny bez DPH nedodané/ých položky/položek zboží za každý i započatý den prodlení až do výše celkové kupní ceny bez DPH nedodané/ nedodaných položky/položek.

2. V případě prodlení prodávajícího s odstraněním vad zboží, uplatněných v záruční době dle čl. VII. odst. 4. této smlouvy, je kupující oprávněn požadovat po prodávajícím zaplacení smluvní pokuty ve výši 1 000,- Kč za každý i započatý den prodlení až do podpisu protokolu o odstranění vady, nebo do doby uplatnění postupu v souladu s čl. VII. odst. 5. této smlouvy.

3. V případě nedodržení termínu splatnosti faktury vystavené prodávajícím, je prodávající oprávněn požadovat po kupujícím úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení s úhradou faktury.

4. Právo fakturovat a vymáhat smluvní pokutu a úrok z prodlení vzniká kupujícímu prvním dnem následujícím po marném uplynutí doby určené jako čas k plnění a prodávajícímu prvním dnem následujícím po marném uplynutí doby splatnosti faktury.

5. Smluvní pokuty a úrok z prodlení jsou splatné do 30 dnů ode dne doručení písemného oznámení o jejich uplatnění.

6. Smluvní strany se dohodly, že zaplacením smluvní pokuty není dotčeno právo na náhradu vzniklé majetkové či nemajetkové újmy v plné výši, a to tedy i ve výši přesahující vyúčtovanou, resp. uhrazenou smluvní pokutu, a rovněž není dotčeno plnit řádně povinnosti vyplývající z této smlouvy.

7. Smluvní pokutu a náklady dle odst. 5 tohoto článku je kupující oprávněn započíst proti částce fakturované prodávajícím s tím, že kontaktní osoba kupujícího bude o případné výši smluvní pokuty resp. nákladů informovat elektronicky kontaktní osobu prodávajícího. Prodávající podpisem této smlouvy uděluje k takovému postupu souhlas.

IX. Zvláštní ujednání

1. Prodávající prohlašuje, že zboží není zatíženo právy třetích osob.

2. Prodávající potvrzuje, že se plně seznámil s rozsahem a povahou dodávky týkající se předmětu výše uvedené Veřejné zakázky, a že jsou mu známy veškeré technické, kvalitativní a jiné podmínky dodávky.

3. Prodávající se zavazuje zachovávat mlčenlivost ohledně všech skutečností, se kterými se seznámí při plnění této smlouvy. Tato povinnost zavazuje i zmocněnce, zaměstnance nebo jiné pomocníky prodávajícího, kteří se podílejí na plnění této smlouvy.

4. Práva a povinnosti vyplývající z této smlouvy ani celou tuto smlouvu nemůže žádná ze smluvních stran převést anebo postoupit na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany.

5. Obě smluvní strany jsou povinny si bez zbytečného odkladu sdělit písemně veškeré skutečnosti, které se dotýkají změn některého z jejich základních identifikačních údajů nebo kontaktních údajů včetně právního nástupnictví.

6. Smluvní strany vylučují přijetí této smlouvy s jakoukoliv odchylkou, byť by to byla odchylka, která podstatně nemění původní podmínky. Totéž platí i pro sjednávání jakýchkoliv změn této smlouvy.

7. Ustanovení této smlouvy je třeba vykládat v souladu se zadávacími podmínkami k Veřejné zakázce, zejména podmínkami stanovenými v zadávací dokumentaci Veřejné zakázky a v souladu s nabídkou prodávajícího.

8. Kupující je oprávněn, resp. stanoví-li tak právní předpis, povinen, uzavřenou smlouvu zveřejnit v souladu s právními předpisy a prodávající s tímto souhlasí.

9. Prodávající se zavazuje spolupůsobit při výkonu finanční kontroly. Podle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, v platném znění, je prodávající osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží z veřejných výdajů nebo z veřejné finanční podpory. Prodávající se zavazuje stejným způsobem zavázat i svoje poddodavatele.

10. Prodávající je povinen uchovávat všechny doklady a dokumenty po dobu a způsobem stanoveným platnými právními předpisy (zákon č. 563/1991 Sb., o účetnictví, v platném znění a zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, v platném znění).

11. Smluvní strany se dohodly, že všechny závazné projevy vůle je třeba činit písemnou formou a prokazatelně doručit druhé smluvní straně na adresu sídla uvedenou v úvodních ustanoveních této smlouvy s výjimkou případů v této smlouvě uvedených, kdy postačuje elektronická forma. Pokud smluvní strana, které je písemnost adresována, její přijetí odmítne nebo jiným způsobem zmaří, má se za to, že zásilka odeslaná s využitím provozovatele poštovních služeb došla třetí pracovní den po odeslání, byla-li však odeslána na adresu v jiném státu, pak patnáctý pracovní den po odeslání. Pokud je na doručení druhé smluvní straně vázán počátek běhu doby určené touto smlouvou a smluvní strana, které je písemnost adresována, její přijetí odmítne nebo jiným způsobem zmaří, počíná taková doba běžet následujícího dne po uplynutí třetího pracovního dne ode dne od uložení písemnosti na poště. Toto však neplatí, využije-li některá ze smluvních stran

pro doručení písemnosti datovou schránku ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v platném znění.

12. Kupující deklaruje a prodávající bere na vědomí, že kupující není ve vztazích vyplývajících z této smlouvy podnikatelem.

13. Je-li prodávajícím více dodavatelů v případě společné účasti ve Veřejné zakázce, nesou všichni tito dodavatelé společně a nerozdílně odpovědnost za plnění této smlouvy.

X. Zánik závazků

1. Zánik závazků z této smlouvy se řídí příslušnými ustanoveními OZ a touto smlouvou.

2. Smluvní strany se dohodly, že podstatným porušením smlouvy ve smyslu § 2002 odst. 1 OZ se vedle případů specifikovaných v § 2002 OZ rozumí také:
   a) prodlení prodávajícího s dodáním zboží (či jeho části) a/nebo s jeho instalací a/nebo s jeho zprovozněním v dohodnutém termínu dle čl. III. odst. 2. této smlouvy delší než 30 kalendářních dnů;
   b) prodlení kupujícího s uhrazením kupní ceny delší než 30 kalendářních dnů, přičemž prodávající je povinen před odstoupení od smlouvy kupujícího písemně upozornit na neplnění jeho závazků a poskytnout mu přiměřenou lhůtu k nápravě;
   c) nedodržení sjednaného množství, jakosti nebo druhu zboží;
   d) jestliže zboží nemá vlastnosti deklarované prodávajícím v této smlouvě či vlastnosti z této smlouvy vyplývající, příp. není v souladu se specifikací zboží;
   e) jestliže prodávající ve své nabídce v rámci Veřejné zakázky, která předcházela uzavření této smlouvy, uvedl informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek zadávacího řízení.

3. Odstoupení od této smlouvy musí být písemné a nabývá účinnosti dnem doručení tohoto písemného oznámení druhé smluvní straně.

4. V případě odstoupení od této smlouvy jsou smluvní strany povinny vypořádat své vzájemné závazky a pohledávky stanovené v zákoně nebo v této smlouvě, a to do 30 dnů od právních účinků odstoupení nebo v dohodnuté lhůtě.

5. Ukončením účinnosti této smlouvy odstoupením od smlouvy nebo jiným způsobem nejsou dotčena práva na smluvní pokuty a náhradu újmy a další závazky, z jejichž povahy vyplývá, že mají trvat i po ukončení účinnosti této smlouvy.

XI. Závěrečná ujednání

1. V otázkách touto smlouvou výslovně neupravených se práva a povinnosti smluvních stran řídí příslušnými ustanoveními obecně závazných právních předpisů platných na území České republiky, zejména OZ, ZZVZ a ostatními právními předpisy vztahujícími se k předmětu této smlouvy.

Univerzita Pardubice

2. Veškeré spory, které se smluvním stranám nepodaří vyřešit smírnou cestou, budou řešeny věcně a místně příslušným soudem České republiky.

3. Tato smlouva bude uzavřena v elektronické nebo listinné podobě, v závislosti na možnostech a dohodě smluvních stran.
   a) V případě uzavření v listinné podobě bude vyhotovena ve čtyřech stejnopisech, z nichž každý má platnost originálu a každá smluvní strana obdrží po dvou z nich.
   b) V případě uzavření v elektronické podobě bude uzavřena připojením uznávaných elektronických podpisů obou smluvních stran.

   Toto ustanovení se použije obdobně i na případné dodatky smlouvy.

4. Tato smlouva může být měněna či doplňována pouze písemnými, oboustranně dohodnutými, vzestupně číslovanými dodatky v souladu se ZZVZ, které se stávají její nedílnou součástí. Za písemnou formu není pro tento účel považována výměna e-mailových či jiných elektronických zpráv. Neplatnost dodatků z důvodu nedodržení formy lze namítnout kdykoliv, a to i když již bylo započato s plněním. Za změnu smlouvy se nepovažuje změna identifikačních či kontaktních údajů.

5. Pokud bude z jakéhokoliv důvodu některé ustanovení této smlouvy shledáno neplatným, nečiní tato skutečnost neplatnou celou smlouvu. V takovém případě jsou smluvní strany povinny bez zbytečného odkladu neplatné ustanovení nahradit novým platným, jenž bude odpovídat smyslu a účelu této smlouvy.

6. Tato smlouva nabývá platnosti dnem podpisu smluvních stran, účinnosti dnem zveřejnění 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), v platném znění.

7. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně, na důkaz čehož připojují oprávnění zástupci smluvních stran své podpisy.

8. Nedílnou součástí této smlouvy jsou následující přílohy:

   Příloha č. 1: Technická specifikace
   Příloha č. 2: Výkaz výměr (položkový rozpočet)
   Příloha č. 3: Závazně používané standardy

V Pardubicích dne
za kupujícího

prof. Ing. Tatiana Molková, Ph.D.
Digitálně podepsal prof. Ing. Tatiana Molková, Ph.D.
Datum: 2020.04.24 13:40:10 +02'00'

prof. Ing. Jiří Málek, DrSc.
rektor

V Brně dne
za prodávajícího

[redacted]
Digitálně podepsal [redacted]
Datum: 2020.04.27 12:28:02 +02'00'

[redacted]
jednatel

Univerzita Pardubice

TECHNICKÁ SPECIFIKACE

DODÁVKA BEZPEČNOSTNÍ INFRASTRUKTURY

VERZE 1.0 20191016

OBSAH

1. OBECNÁ FUNKČNÍ A TECHNICKÁ SPECIFIKACE

1.1. POPIS POŽADOVANÉHO ŘEŠENÍ

Předmětem plnění je rozšíření stávající bezpečnostní infrastruktury dodávkou nových bezpečnostních zařízení, licencí a software pro centrální správu jednotlivých částí bezpečnostní infrastruktury a poskytnutí služeb:

- Auditu současného nastavení
  - perimetrových firewallů včetně VPN funkcionality
  - Internet brány a jádra sítě
  - bezpečnostního přístupového systému

- Vyhotovení technické dokumentace, která bude podléhat odsouhlasení odpovědným zástupcem Zadavatele
- Dodávku 3 ks nových zařízení třídy Next generation firewall, dále jen NGFW, které musí být možné provozovat v clusteru (režim vysoké dostupnosti) se stávajícím zařízením Cisco Firepower 4110.
- Implementace systému v reřimu vysoké dostupnosti HA
- Dodávku a implementaci 2 ks licencí IPS pro NGFW s podporu na dobu 3 let od uzavření smlouvy, která zajistí pravidelné updatování IPS signatur a bezpečnostních databází.
- Dodávku a implementace centralizovaného management nástroje, který umožní centralizovanou správu, jak stávajícího bezpečnostního zařízení Cisco Firepower 4110, tak 3 ks nově dodaných zařízení.
- Dodávku a implementaci licencí pro zabezpečení vzdáleného přístupu do KI UPa pro 1000 uživatelů současně.
- Migrace současného nastaveni firewallů pro nový systém NGFW včetně VPN funkcionality.
- Integrace nového systému NGFW do stávajících bezpečnostních a informačních systémů
- Provedení korekcí/oprav současného nastavení bezpečnostního přístupového systému, bude-li to potřeba
- Provedení korekcí/oprav současného nastaveni Internet brány a jádra sítě, bude-li to potřeba
- Optimalizace nastavení nového systému NGFW
- Provedení finální korekce/opravy technické dokumentace a její předání Zadavateli

Pokud tato Technická specifikace neurčí jinak, musí být nabízené technologie v souladu s platnými standardy UPa, které jsou nedílnou součástí této zadávací dokumentace v příloze č. 5 „Závazně používané standardy datových sítí“. Pokud jsou některé parametry požadované v této Technické specifikaci v rozporu s přílohou č. 5 zadávací dokumentace, účastník zadávacího řízení (dále jen „účastník“) jako závazné bere parametry uvedené v této Technické specifikaci.

Veškerá zařízení nabízená účastníkem v rámci tohoto výběrového řízení musí být určena pro český trh a koncového zákazníka Univerzita Pardubice. Zadavatel požaduje originální a nové zařízení, licencované ve jménu zákazníka tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.

U vybraných zařízení bude vybraný dodavatel, v průběhu poskytovaného plnění vyplývajícího z následné smlouvy, povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení) pro český trh a koncového zákazníka Univerzita Pardubice, pokud o to zadavatel požádá.

Z důvodu kompatibility zadavatel požaduje, aby veškerý HW a SW dodávaný v rámci tohoto zadávacího řízení byl od jednoho výrobce a byl plně kompatibilní se stávající bezpečnostní infrastrukturou zadavatele.

1.2. POPIS CELKOVÉ IMPLEMENTACE

Zadavatel rozdělil realizaci předmětu veřejné zakázky do Čtyř fází:

1. Audit a vyhotovení technické dokumentace.

2. Dodávka nových hardwarových a softwarových prvků a jejich fyzická instalace.

3. Přechod na nový systém NGFW.

4. Optimalizace nového systému NGFW včetně případné korekce/opravy projektové dokumentace.

1.3. PODMÍNKY PRO TECHNICKÉ SPLNĚNÍ JEDNOTLIVÝCH FÁZÍ

Fáze č. I - Audit a vyhotovení technické dokumentace

- Audit současného nastavení perimetrových firewaltů (včetně VPN funkcionality), INTERNET brány a jádra sítě a bezpečnostního přístupového systému
- Příprava zadání technické dokumentace na základě auditu
- Vyhotovení technické dokumentace*
- Schválení technické dokumentace Zadavatelem

*) Technická dokumentace musí obsahovat min. následující:

- Návrh topologie a fyzického zapojení dodávaných systémů do infrastruktury UPa
- Návrh konfigurace a nastaveni NGFW (včetně VPN funkcionality) a IPS
- Na základě výsledků auditu návrh změny nastavení u spolupracujících systémů (IPS, Internet brány, jádro sítě atd.
- Zálohování
- Návrh na akceptačnítesty

Fáze č. II - Dodávka nových hardwarových a softwarových prvků a fyzická instalace NGFW

- Dodávka tří firewallů nové generace NGFW včetně poskytnutí provozních licencí na dobu 36 měsíců, bude-li to s ohledem na nabízené řešení vyžadováno
- Implementace systému NGFW v režimu vysoké dostupnosti HA
- Konverze nastavení současného firewallu CISCO ASA5585-20 do NGFW

Fáze č. III - Přechod na nový systém NGFW

- Migrace současného nastavení firewallů pro nový systém NGFW
- Konfigurace VPN včetně distribuce a nasazeníVPN klientů
- Implementace IPS
- Integrace nového systému NGFW do stávajících bezpečnostních a informačních systémů.
- Zabezpečení pravidelných záloh konfigurací NGFW
- Korekce/oprava nastavení bezpečnostního přístupového systému
- Korekce/oprava nastavení Internet brány a jádra sítě
- Přenos provozu na nový systém NGFW

Fáze č. IV - Optimalizace nového systému NGFW včetně případné korekce/opravy projektové dokumentace

- Monitoring stavu nového systému NGFW alespoň v délce 3 měsíců.
- Optimalizace a oprava chyb (pokud je to třeba) nastavení nového systému NGFW.
- Finální korekce/oprava technické dokumentace a její předáni Zadavateli.

1.4. DOBA PLNĚNÍ VEŘEJNÉ ZAKÁZKY A ODHADOVANÁ ČASOVÁ NÁROČNOST PRO SPLNĚNÍ JEDNOTLIVÝCH FÁZÍ

p.č.	Jednotlivé fáze implementace	MD
1.0	**Fáze č.I - Audit a vyhotovení projektové dokumentace**	
1.1	Audit současného nastavení perimetrových firewallů (včetně VPN funkcionality), Internet Brány a jádra sítě a pezpečnostního přístupového systému	15
1.2	Vyhotovení technické dokumentace	5
	Celkem	20
2.0	**Fáze č.II - Dodávka nových hw a sw prostředků a fyzická instalace NGFW**	
2.1	Implementace systému NGFW v režimu vysoké dostupnosti HA	4
2.2	Konverze současného firewallu do NGFW	4
	Celkem	8
3.0	**Fáze č.III - Přechod na nový systém NGFW**	
3.1	Migrace současného nastavení firewallů na nový systém NGFW včetně VPN	5
3.2	Implementace IPS	5
3.3	Integrace nového systémů NGFW do stávajících bezpečnostních a informačních systémů	4
3.4	Zabezpečení pravidelných záloh konfigurací NGFW	1
3.5	Korekce/oprava nastavení bezpečnostního přístupového systému, Internet brány a jádra sítě.	5
3.6	Přenos provozu na nový systém NGFW	4
	Celkem	24
4.0	**Fáze č.IV - Optimalizace nového systému NGFW**	
4.1	Monitoring stavu nového systému NGFW během 3 měsíců (dohromady - sledování provozu)	6
4.2	Optimalizace a oprava chyb nastavení nového systému NGFW	2
4.3	Finální korekce/oprava technické dokumentace	5
	Celkem	13
	Celkový počet MD	**65**

2. CENTRÁLNÍ CLUSTER NGFW

Požadujeme dodání 3 ks zařízení třídy Next Generation Firewall (NGFW), které bude možné provozovat v režimu vysoké dostupnosti (hight availability cluster) se stávajícím zařízením firewallem Cisco Firepower 4110. Zařízení musí disponovat redundantními zdroji napájení a dalšími vlastnostmi popsanými v kapitole 2.1.

2.1. HARDWARE ZAŘÍZENÍ VČETNĚ SOFTWARE

Počet kusů – 3

Součástí dodávky musí být i následující počet originálních modulů výrobce pro připojení dodávaných zařízení do komunikační infrastruktury Zadavatele:

- 3 ks 1000BASE-T
- 14 ks 10GBASE-CU - twinax kabel opatřený na obou stranách koncovkami pro SFP+ délky 10 metrů
- 4 ks 10GBASE-SR
- 12 ks 10GBASE-LR

Zařízení musí splňovat následující parametry:

Výkon a funkcionalita firewallu:

- Musí být možné provozovat zařízení v HA se stávajícím zařízením Firepower 4110
- Formát zařízení - Appliance, 1RU
- Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených - 1
- Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených - 8
- Možnost rozšíření o moduly rozhraní - 2
- Možnost rozšíření o další 10Gb SFP+ rozhraní - 8
- Možnost rozšíření o další 40Gb SFP+ rozhraní - 4
- Redundantní zdroje
- Podporovaný počet současně otevřených spojení NGFW s AVC - 10M
- Rychlost vytváření nových spojení NGFW s AVC - 64K
- Propustnost stavového FW (top parametry) - 35 Gbps
- Propustnost NGIPS (top parametry) - 15 Gbps
- Propustnost aplikačního FW (next-gen FW) – (top parametry) - 13 Gbps
- Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry) - 11 Gbps
- Hardwarové dešifrování TLS - 4,5 Gbps
- Podpora L2 (transparentního) módu s podporou NAT a PAT
- Podpora L3 (routovaného) módu s podporou NAT a PAT
- Podporovaný počet VLAN - Min. 1024
- Podpora stateful failover - active/standby
- Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru podpora min. 6 šasi
- Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru
- Podpora min. 3 virtuálních bezpečnostních kontextů (virtuálních firewallů)
- Dynamické směrování - podpora alespoň RIP, OSPF, BGP
- Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP
- Podpora Policy based Routing
- Podpora kontroly paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.
- Podpora filtrace IPv4, IPv6
- Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD

- Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích
- Podpora inspekce IPv6 provozu
- Podpora NAT64 a DNS64
- Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.
- Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ
- Možnost rozšíření o funkce NextGen FW
- Možnost rozšíření o funkce NextGen IPS
- Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele
- Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech
- API rozhraní pro sdílení kontextových informací s dalšími systémy
- Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)

2.2. SERVISNÍ PODPORA A PRODLOUŽENÍ ZÁRUKY OD VÝROBCE

Účastník je povinen v rámci dodávky zajistit podporu všech dodaných produktů (hardware i software), a to za podmínek uvedených v kapitole 6.1 SERVISNÍ SLUŽBY NA NOVĚ DODÁVANÉ AKTIVNÍ A SOFTWARE KOMPONENTY.

3. IPS LICENCE

Požadujeme dodání IPS licencí pro 2 ks NGFW. Licence musí být využitelné, jak na kterémkoliv z dodávaných zařízení, tak na stávajícím zařízení Cisco Firepower 4110. Dodané IPS licence musí zajistit rozšíření NGFW o vlastnosti popsané v kapitole 3.1.

Jestliže splnění kritérií popsaných níže vyžaduje zakoupení speciální licence, pak zadavatel požaduje, aby v ceně nabízeného řešení byla licence na tyto funkcionality platná na 3 roky.

3.1. HARDWARE ZAŘÍZENÍ VČETNĚ SOFTWARE

2 ks zařízení, na nichž bude IPS funkcionalita zapnuta, musí splňovat následující parametry:

Funkce IPS:

- Možnost definovat typ provozu předávaný k inspekci do IPS
- Podpora také IDS režimu – pasivního monitorování (TAP režim)
- Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)
- Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti
- Security intelligence feeds na báze FQDN
- Podpora 802.1Q tagovaných rámců
- Podpora různých IPS politik pro různé typy provozu
- Inspekce pro IPv4 i IPv6
- Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému
- 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
- Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací
- Podpora aplikace pro psaní zákaznických filtrů
- Podpora importu komunitních filtrů/signatur Snort
- IPS musí umět detekovat a blokovat útoky průzkumných aktivit
- IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS
- 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
- 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
- Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události
- Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku
- Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive
- Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí
- Možnost definice uživatelské vrstvy politik
- Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik
- Různé politiky lze sdílet a aplikovat na různé senzory
- Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů
- Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry
- IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků

- Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“
- Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.
- Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.
- Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly
- Podpora databází reputací adres v Internetu (Security Intelligence)

3.2. SERVISNÍ PODPORA A PRODLOUŽENÍ ZÁRUKY OD VÝROBCE

Účastník je povinen v rámci dodávky zajistit podporu všech dodaných produktů (hardware i software), a to za podmínek uvedených v kapitole 6.1 SERVISNÍ SLUŽBY NA NOVĚ DODÁVANÉ AKTIVNÍ A SOFTWARE KOMPONENTY.

4. REMOTE ACCESS VPN

Pro zabezpečení vzdáleného přístupu do KI UPa požadujeme dodávku licencí pro 1000 současně přistupujících uživatelů minimálně na 3 roky. Licence musí být využitelné, jak na kterémkoliv z dodávaných zařízení, tak na stávajícím zařízení Cisco Firepower 4110.

4.1. HARDWARE ZAŘÍZENÍ VČETNĚ SOFTWARE

Nabízený software musí splňovat následující vlastnosti:

- Počet licencí VPN klienta na 3 roky pro požadovaný NGFW a používaný Firepower 4110 - 1000
- Podpora IPSec VPN
- 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
- Podpora nového protokolu pro výměny klíčů IKEv2
- Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256
- Podpora kontrolních mechanizmů: MD5, SHA
- Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256
- Podpora komponentu Suite-B: SHA-2 mechanizmu s metodami: SHA-256, SHA-384
- Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA
- Podpora SSL VPN
- Jednotný klient pro IPsec (IKEv2) i SSL VPN
- 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
- 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
- VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)
- VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů
- SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS.
- Podora TLS i DTLS pro SSL připojení
- Podpora současné autentizace koncové stanice i uživatele
- Podpora definice pravidel pro VPN přístup přímo prostředky FW a jejich automatická distribuce VPN připojeným klientům
- Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů
- Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)
- Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačnícho systému
- Podpora autentizačních mechanizmů: lokální databáze na FW, RADIUS, Lightweight Directory Access Protocol (LDAP)
- Podpora veřejných CA, včetně možnosti CA přímo na firewallu
- Možnost současné autentizace AAA a certifikátem

4.2. SERVISNÍ PODPORA A PRODLOUŽENÍ ZÁRUKY OD VÝROBCE

Účastník je povinen v rámci dodávky zajistit podporu všech dodaných produktů (hardware i software), a to za podmínek uvedených v kapitole 6.1 SERVISNÍ SLUŽBY NA NOVĚ DODÁVANÉ AKTIVNÍ A SOFTWARE KOMPONENTY.

5. CENTRÁLNÍ MANAGEMENT NGFW

Pro zajištění centrální správy a ukládání logů ze stávajícího zařízení Cisco Firepower 4110 a nově dodávaných zařízení požadujeme 1 ks HW appliance a software pro centralizovanou správu.

Nabízený software musí splňovat parametry popsané v kapitole 5.1.

Součástí dodávky musí být i následující počet originálních modulů výrobce pro připojení dodávaných zařízení do komunikační infrastruktury Zadavatele:

- 2 ks 10GBASE-SR

5.1. HARDWARE ZAŘÍZENÍ VČETNĚ SOFTWARE

Nabízené zařízení musí splňovat následující vlastnosti:

Základní vlastnosti:

- Třída zařízení – HW appliance včetně SW
- Formát zařízení - fixní 1RU
- Centralizovaný management pro stávající a nově poptávané firewallové řešení nové generace popsané v kapitole 1.2
- Minimální počet podporovaných zařízení - 300
- Paměť RAM – 64 Gbps
- Počet a typ síťových rohraní - 2 x 1 Gbps RJ45 a 2x 10Gbps SFP+
- Velikost paměti pro uchovávání bezpečnostních incidentů – 1.8 TB
- Minimální FPS (flows per seconds) rate – 12 000
- Redundantní zdroje napájení

Správa:

- Jednotná správa poptávaných 3ks Next-Gen FW a současného Firepower 4110
- Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW
- Přístup ke GUI http/https protokolem
- Možnost vzdáleného přístupem protokolem ssh přímo do FW
- Možnost přístupu k textovým logům (syslog) přímo ve FW
- Možnost centrální správy při nasazení více firewallů
- Při centrální správě: možnost sdílených bezpečnostních politik
- Při použití clusteru se spravuje pouze jeden logický prvek
- Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu
- Zobrazení logů a událostí v grafickém rozhraní správy
- 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.
- Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování
- Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, 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.
- Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu
- Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole

- Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic
- Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu
- Pro reporty lze definovat template definující formát a obsah reportu
- Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu
- V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N
- Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů
- Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.
- Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.
- Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay
- Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu
- Podpora řízeného přístupu podle rolí administrátorů
- Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora
- Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu
- Workflow pro předávání „ticketů“ mezi administrátory
- Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu
- Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)
- Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“
- Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli
- Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.
- Podpora pasivního monitorování (TAP režim)
- Podpora 802.1Q tagovaných rámců
- Podporovaných aplikací – min. 3000
- Kategorie aplikací (nebezpečné, důležité, apod.)
- Filtrace podle typů aplikací webových i ne-webových
- SSL inspekce (dekrypce/enkrypce)
- Filtry mohou zohlednit roli a identitu uživatele
- Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)
- Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě
- 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
- 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
    - 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
- Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.
- Podpora posílání událostí formou syslog, email, SNMP na externí platformy
- Podpora Event Streamer API (eStreamer) pro sdílení informací s externími systémy. Minimálně pro tyto SIEM:
    - ArcSight
    - BMC Remedy
    - Trustwave
    - NetForensics
    - Novell Sentinel
    - Hawk Network Defense
    - Q1Labs-QRadar
    - Log Rhythm SIEM 2.0
    - LogLogic
    - Splunk

5.2. SERVISNÍ PODPORA A PRODLOUŽENÍ ZÁRUKY OD VÝROBCE

Účastník je povinen v rámci dodávky zajistit podporu všech dodaných produktů (hardware i software), a to za podmínek uvedených v kapitole 6.1 SERVISNÍ SLUŽBY NA NOVĚ DODÁVANÉ AKTIVNÍ A SOFTWARE KOMPONENTY.

6. ZAJIŠTĚNÍ SERVISNÍCH SLUŽEB

6.1. SERVISNÍ SLUŽBY NA NOVĚ DODÁVANÉ AKTIVNÍ A SOFTWARE KOMPONENTY

Účastník je povinen v rámci dodávky zajistit minimálně 3 letou podporu všech dodaných produktů, a to za následujících podmínek:

- Účastník poskytne zadavateli po dobu trvání podpory (3 roky) všechny relevantní SW releases a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání zadavatele a fungovalo bez závad. Účastník 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. Účastník se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Účastník je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízeni tak, aby v případě závady na dodaných zařízeních, kterou není účastník schopen sám odstranit, bylo možné eskalovat závadu přímo k výrobci zařízení. Zároveň je účastník povinen zajistit zadavateli přistup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- Účastník je povinen zajistit opravu pro dodané řešení za podmínek specifikovaných zadavatelem v režimu 24x7 po dobu 3 let. Odstranění závady do 24 hodin od nahlášení závady.
- Výše specifikovanou podporu a dostupnost náhradních dílů zadavatel požaduje po dobu min. 3 let.
- Záruka na HW a SW 3 roky (od výrobce)
- Při reklamačním procesu zůstává vadné zboží u zákazníka
- Bezplatný přístup k novým verzím firmware po dobu 3 roků
- Řešení složitějších technických problémů v češtině pomocí lokálního partnera výrobce nabízených technologií.
- Dodavatel zajistí seznámení zástupců objednatele s nástroji pro centrální správu, s funkcemi administrátorského přístupu k nástrojům jednotlivých funkcí, se zabezpečeným přístupem pro vzdálenou správu jednotlivých komponent (https, ssh), s grafickým rozhraním pro správu jednotlivých komponent řešení, s nástroji pro hromadné a dávkové konfigurace a s nástroji pro monitorování technických parametrů systému.

7. OSTATNÍ

V případě, že tato technická specifikace obsahuje požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku, za příznačné, patenty, ochranné známky nebo označení původu, umožňuje zadavatel pro plnění veřejné zakázky použití i jiných, kvalitativně a technicky obdobných řešení.

8. PŘÍLOHY

8.1. ZÁVAZNÉ TECHNICKÉ A FUNKČNÍ POŽADAVKY

Tabulky plnění závazných technických a funkčních požadavků zadavatele k vyplnění pro účastníka.

Účastník vyplní tabulky v poli „hodnota nabízená účastníkem“ a v poli „odkaz na produktovou dokumentaci účastníka“.

Pole ve sloupci „minimální požadovaná hodnota zadavatelem“ může obsahovat tyto údaje:

- PODPORUJE = je součástí zařízení; v takovém případě účastník splní požadavek zadavatele, pokud s ohledem na jeho nabídku uvede do sloupce „hodnota nabízená účastníkem“ údaj „PODPORUJE“
- UMOŽŇUJE = funkcionalitu lze v budoucnu aktivovat upgradem SW, licenčně nebo instalací dalšího HW přímo do zařízení; v takovém případě účastník splní požadavek zadavatele, pokud s ohledem na jeho nabídku uvede do sloupce „hodnota nabízená účastníkem“ údaj „UMOŽŇUJE“
- Jiný požadavek zadavatele na uvedení číselného údaje, rozmezí či podobně; v takovém případě účastník splní požadavek zadavatele, pokud s ohledem na jeho nabídku uvede do sloupce „hodnota nabízená účastníkem“ parametr dle požadavku zadavatele

Pole ve sloupci „odkaz na produktovou dokumentaci účastníka“ účastník vyplní názvem či jinou jednoznačnou identifikací dokumentu, která takovou produktovou dokumentaci ve vztahu k tomu kterému parametru obsahuje (například produktový list, katalogový list, datasheet, část instalačního či jiného manuálu apod.).

Produktovou dokumentaci účastníka (sadu dokumentů) souhrnně vloží pod doplněnou Tabulky plnění závazných technických a funkčních požadavků zadavatele.

Plnění závazných technických a funkčních požadavků na obnovu a vybudování nových částí sítě s odkazy na produktovou dokumentaci u nabízených SW, HW a pasivních komponent.

	Parametr/funkcionalita	minimální hodnota požadovaná zadavatelem	hodnota nabízená účastníkem	odkaz na produktovou dokumentaci účastníka
CENTRÁLNÍ HA CLUSTER NGFW				
1.	Musí být možné provozovat 3 ks nových zařízení v HA se stávajícím zařízením Firepower 4110	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
2.	Formát zařízení - Appliance, 1RU	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
3.	Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1	1	FPWR_4110_datasheet.pdf
4.	Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	8	8	FPWR_4110_datasheet.pdf
5.	Možnost rozšíření o moduly rozhraní	2	2	FPWR_4110_datasheet.pdf

6.	Možnost rozšíření o další 10Gb SFP+ rozhraní	8	8	FPWR_4110_datasheet.pdf
7.	Možnost rozšíření o další 40Gb SFP+ rozhraní	4	4	FPWR_4110_datasheet.pdf
8.	Redundantní zdroje	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
9.	Podporovaný počet současně otevřených spojení NGFW s AVC	10M	10M	FPWR_4110_datasheet.pdf
10.	Rychlost vytváření nových spojení NGFW s AVC	64K	64K	FPWR_4110_datasheet.pdf
11.	Propustnost stavového FW (top parametry)	35 Gbps	35 Gbps	FPWR_4110_datasheet.pdf
12.	Propustnost NGIPS (top parametry)	15 Gbps	15 Gbps	FPWR_4110_datasheet.pdf
13.	Propustnost aplikačního FW (next-gen FW) – (top parametry)	13 Gbps	13 Gbps	FPWR_4110_datasheet.pdf
14.	Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	11 Gbps	11 Gbps	FPWR_4110_datasheet.pdf
15.	Hardwarové dešifrování TLS	4,5 Gbps	4,5 Gbps	FPWR_4110_datasheet.pdf
16.	Podpora L2 (transparentního) módu s podporou NAT a PAT	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
17.	Podpora L3 (routovaného) módu s podporou NAT a PAT	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
18.	Podporovaný počet VLAN	Min. 1024	Min. 1024	firepower-config-guide-v63.pdf
19.	Podpora stateful failover active/standby	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
20.	Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru podpora min. 6 šasi	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
21.	Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
22.	Podpora min. 3 virtuálních bezpečnostních kontextů (virtuálních firewallů)	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
23.	Dynamické směrování - podpora alespoň RIP, OSPF, BGP	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
24.	Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
25.	Podpora Policy based Routing	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
26.	Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
27.	Podpora filtrace IPv4, IPv6	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
28.	Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
29.	Podpora filtrace podle bezpečnostních skupinových rolí	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf

	přiřazených na přístupových přepínačích			
30.	Podpora inspekce IPv6 provozu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
31.	Podpora NAT64 a DNS64	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
32.	Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
33.	Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
34.	Možnost rozšíření o funkce NextGen FW	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
35.	Možnost rozšíření o funkce NextGen IPS	PODPORUJE	PODPORUJE	FPWR_4110_datasheet.pdf
36.	Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
37.	Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
38.	API rozhraní pro sdílení kontextových informací s dalšími systémy	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
39.	Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	PODPORUJE	PODPORUJE	FTD-APIC-integration.pdf
	IPS LICENCE			
1.	Možnost definovat typ provozu předávaný k inspekci do IPS	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
2.	Podpora také IDS režimu – pasivního monitorování (TAP režim)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
3.	Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
4.	Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
5.	Security intelligence feeds na báze FQDN	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
6.	Podpora 802.1Q tagovaných rámců	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
7.	Podpora různých IPS politik pro různé typy provozu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
8.	Inspekce pro IPv4 i IPv6	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
9.	Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
10.	IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry,	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf

	průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií			
11.	Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
12.	Podpora aplikace pro psaní zákaznických filtrů	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
13.	Podpora importu komunitních filtrů/signatur Snort	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
14.	IPS musí umět detekovat a blokovat útoky průzkumných aktivit	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
15.	IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
16.	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	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
17.	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	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
18.	Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
19.	Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
20.	Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
21.	Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
22.	Možnost definice uživatelské vrstvy politik	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
23.	Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
24.	Různé politiky lze sdílet a aplikovat na různé senzory	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
25.	Podpora aktivní inline ochrany před malware s detekcí známých	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf

	nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů			
26.	Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
27.	IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
28.	Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
29.	Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
30.	Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
31.	Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
32.	Podpora databází reputací adres v Internetu (Security Intelligence)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
REMOTE ACCESS VPN				
1.	Podpora IPSec VPN	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
2.	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	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
3.	Podpora nového protokolu pro výměny klíčů IKEv2	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
4.	Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
5.	Podpora kontrolních mechanizmů: MD5, SHA	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
6.	Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
7.	Podpora komponentu Suite-B: SHA-2 mechanizmu s metodami: SHA-256, SHA-384	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
8.	Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
9.	Podpora SSL VPN	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
10.	Jednotný klient pro IPsec (IKEv2) i SSL VPN	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf

11.	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	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
12.	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	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
13.	VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
14.	VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
15.	SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS.	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
16.	Podora TLS i DTLS pro SSL připojení	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
17.	Podpora současné autentizace koncové stanice i uživatele	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
18.	Podpora definice pravidel pro VPN přístup přímo prostředky FW a jejich automatická distribuce VPN připojeným klientům	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
19.	Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
20.	Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
21.	Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačnícho systému	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
22.	Podpora autentizačních mechanizmů: lokální databáze na FW, RADIUS, Lightweight Directory Access Protocol (LDAP)	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
23.	Podpora veřejných CA, včetně možnosti CA přímo na firewallu	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
24.	Možnost současné autentizace AAA a certifikátem	PODPORUJE	PODPORUJE	Anyconnect_datasheet.pdf
CENTRÁLNÍ MANAGEMENT NGWF				
1.	Jednotná správa 3ks nových zařízení Next-Gen FW a současného Firepower 4110	PODPORUJE	PODPORUJE	FMC_datasheet.pdf

2.	Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
3.	Přístup ke GUI http/https protokolem	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
4.	Možnost vzdáleného přístupem protokolem ssh přímo do FW	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
5.	Možnost přístupu k textovým logům (syslog) přímo ve FW	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
6.	Možnost centrální správy při nasazení více firewallů	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
7.	Při centrální správě: možnost sdílených bezpečnostních politik	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
8.	Při použití clusteru se spravuje pouze jeden logický prvek	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
9.	Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
10.	Zobrazení logů a událostí v grafickém rozhraní správy	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
11.	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.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
12.	Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
13.	Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
14.	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.	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
15.	Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
16.	Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	PODPORUJE	PODPORUJE	FMC_datasheet.pdf

17.	Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
18.	Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
19.	Pro reporty lze definovat template definující formát a obsah reportu	PODPORUJE	PODPORUJE	FMC_datasheet.pdf
20.	Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
21.	V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
22.	Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
23.	Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
24.	Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
25.	Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
26.	Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
27.	Podpora řízeného přístupu podle rolí administrátorů	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
28.	Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
29.	Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
30.	Workflow pro předávání „ticketů“ mezi administrátory	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
31.	Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
32.	Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
33.	Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
34.	Různé politiky pro sledování	PODPORUJE	PODPORUJE	firepower-config-

	„zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli			guide-v63.pdf
35.	Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
36.	Podpora pasivního monitorování (TAP režim)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
37.	Podpora 802.1Q tagovaných rámců	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
38.	Podporovaných aplikací	Min. 3000	4000	FMC_datasheet.pdf
39.	Kategorie aplikací (nebezpečné, důležité, apod.)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
40.	Filtrace podle typů aplikací webových i ne-webových	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
41.	SSL inspekce (dekrypce/enkrypce)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
42.	Filtry mohou zohlednit roli a identitu uživatele	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
43.	Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
44.	Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
45.	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	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
46.	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, 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	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
47.	Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
48.	Podpora posílání událostí formou syslog, email, SNMP na externí platformy	PODPORUJE	PODPORUJE	firepower-config-guide-v63.pdf
49.	Podpora Event Streamer API	PODPORUJE	PODPORUJE	firepower-config-

	(eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM: ArcSight, BMC Remedy, Trustwave, NetForensics, Novell Sentinel, Hawk Network Defense, Q1Labs-QRadar, Log Rhythm SIEM 2.0, LogLogic, Splunk			guide-v63.pdf

8.2. LABORATORNÍ TESTY

Na dodávané technologii mohou být provedeny jakékoli testy nebo jejich libovolná kombinace, které odpovídají požadavkům ze zadávací dokumentace. Testy mohou být provedeny v jakémkoli pořadí a nemusí být provedeny všechny, případně pouze na části dodávané technologie. S ohledem na časovou náročnost budou technologické testy provedeny na technologiích dodavatelů, dle pořadí z první části vyhodnocení a to pouze na technologiích těch dodavatelů, kteří se umístí na předních místech. Testy jsou brány jako prokázání technických parametrů deklarovaných v nabídce.

Dodavatel se zavazuje, poskytnout nutnou součinnost technicky způsobilou obsluhou pro nastavení dodávané technologie pro potřeby testování dané technologie.

Ke každému uskutečněnému testu bude vyhotoven protokol, ze kterého bude patrné, jestli byl test splněn či nikoli. Při negativním výsledku testu bude v protokolu popsáno, v jakých parametrech technologie nevyhověla testu.

Nesplnění jakéhokoli testu je chápáno jako nesplnění požadavků ze zadávací dokumentace.

Pro příklad uvádíme výčet možných testů:
switching
- základní vlan a stp
- mac learning
- unicast flooding
- multicast flooding
- broadcast flooding

advanced switching
- test 4096 vlan (core, distribution)
- vlan translation (core, distribution)
- bezpečnost spanning tree

interoperabilita routingu
- základní ospf
- základní ip multicast
- zátěžový test ospf

routing a forwarding
- propustnost ipv4
- propustnost ipv6
- propustnost ip multicast

zákaznické funkce
- bezpečnostní acl na vstupu
- omezování rychlosti na vstupu
- omezování rychlosti na výstupu
- bezpečnostní acl na výstupu
- unicast reverse path forwarding
- acl logging
- netflow
- route flapping test

odolnost proti dos útokům
- brute force dos
- routing dos
- broadcast dos
- ip options dos

Příloha č. 2 Kupní smlouvy č. 1309/19

Výkaz výměr

ver 1.01 20191210

Dodávka bezpečnostní infrastruktury

Pol.	Číslo	Obchodní název	MJ	Počet	Cena/MJ	Celkem	Označení výrobku - typové číslo, výrobce vybrané prvky (*)
1. Centrální HA cluster NGFW							
Hardware zařízení včetně software							
1.	FPR4110-BUN	Cisco Firepower 4110 Master Bundle	ks	1	0 Kč	0 Kč	FPR4110-BUN
2.	FPR4110-NGFW-K9	Cisco Firepower 4110 NGFW Appliance, 1U, 2 x NetMod Bays	ks	1	1 068 826 Kč	1 068 826 Kč	FPR4110-NGFW-K9
3.	FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	ks	1	47 446 Kč	47 446 Kč	FPR4K-PWR-AC-1100
4.	CAB-AC-EUR	Power Cord - Europe, 16/10A,250V, 2500mm, -40C to +85C	ks	2	0 Kč	0 Kč	CAB-AC-EUR
5.	FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	ks	1	0 Kč	0 Kč	FPR4K-SSD200
6.	FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	ks	1	0 Kč	0 Kč	FPR4K-SSD-BBLKD
7.	GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	ks	1	0 Kč	0 Kč	GLC-TE
8.	FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit	ks	1	0 Kč	0 Kč	FPR4K-ACC-KIT
9.	FPR4K-FAN	Firepower 4000 Series Fan	ks	6	0 Kč	0 Kč	FPR4K-FAN
10.	FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	ks	1	0 Kč	0 Kč	FPR4K-PWR-AC-1100
11.	FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	ks	1	0 Kč	0 Kč	FPR4K-RACK-MNT
12.	FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	ks	1	0 Kč	0 Kč	FPR4K-NM-BLANK
13.	FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	ks	1	0 Kč	0 Kč	FPR4K-NM-BLANK
14.	SFP-10G-AOC10M	10GBASE Active Optical SFP+ Cable, 10M	ks	6	3 088 Kč	18 528 Kč	SFP-10G-AOC10M
15.	SFP-10G-SR-S	10GBASE-SR SFP Module, Enterprise-Class	ks	1	8 314 Kč	8 314 Kč	SFP-10G-SR-S
16.	SFP-10G-LR-S	10GBASE-LR SFP Module, Enterprise-Class	ks	1	23 754 Kč	23 754 Kč	SFP-10G-LR-S
17.	SF-F4KFXOS2.4.1-K9	Cisco Firepower Extensible Operating System v2.4.1 - FPR4100	ks	1	0 Kč	0 Kč	SF-F4KFXOS2.4.1-K9
18.	SF-F4K-TD6.3-K9	Cisco Firepower Threat Defense software v6.3 for FPR4100	ks	1	0 Kč	0 Kč	SF-F4K-TD6.3-K9
19.	FPR4110-FTD-HA-BUN	Cisco Firepower 4110 Threat Defense Chss,Subs HA Bundle	ks	1	0 Kč	0 Kč	FPR4110-FTD-HA-BUN
20.	FPR4110-NGFW-K9	Cisco Firepower 4110 NGFW Appliance, 1U, 2 x NetMod Bays	ks	2	1 068 826 Kč	2 137 652 Kč	FPR4110-NGFW-K9
21.	FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	ks	2	47 446 Kč	94 892 Kč	FPR4K-PWR-AC-1100
22.	CAB-AC-EUR	Power Cord - Europe, 16/10A,250V, 2500mm, -40C to +85C	ks	4	0 Kč	0 Kč	CAB-AC-EUR
23.	FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	ks	2	0 Kč	0 Kč	FPR4K-SSD200
24.	FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	ks	2	0 Kč	0 Kč	FPR4K-SSD-BBLKD
25.	GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	ks	2	0 Kč	0 Kč	GLC-TE
26.	FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit	ks	2	0 Kč	0 Kč	FPR4K-ACC-KIT
27.	FPR4K-FAN	Firepower 4000 Series Fan	ks	12	0 Kč	0 Kč	FPR4K-FAN
28.	FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	ks	2	0 Kč	0 Kč	FPR4K-PWR-AC-1100
29.	FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	ks	2	0 Kč	0 Kč	FPR4K-RACK-MNT
30.	FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	ks	2	0 Kč	0 Kč	FPR4K-NM-BLANK
31.	FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	ks	2	0 Kč	0 Kč	FPR4K-NM-BLANK
32.	SFP-10G-AOC10M	10GBASE Active Optical SFP+ Cable, 10M	ks	8	3 088 Kč	24 704 Kč	SFP-10G-AOC10M
33.	SFP-10G-LR-S	10GBASE-LR SFP Module, Enterprise-Class	ks	6	23 754 Kč	142 524 Kč	SFP-10G-LR-S
34.	SF-F4KFXOS2.4.1-K9	Cisco Firepower Extensible Operating System v2.4.1 - FPR4100	ks	2	0 Kč	0 Kč	SF-F4KFXOS2.4.1-K9
35.	SF-F4K-TD6.3-K9	Cisco Firepower Threat Defense software v6.3 for FPR4100	ks	2	0 Kč	0 Kč	SF-F4K-TD6.3-K9
36.	SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	ks	3	8 314 Kč	24 942 Kč	SFP-10G-SR-S=
37.	SFP-10G-LR-S=	10GBASE-LR SFP Module, Enterprise-Class	ks	5	23 754 Kč	118 770 Kč	SFP-10G-LR-S=
Servisní podpora a prodloužení záruky od výrobce							
1.		Servisní podpora, prodloužení záruky na 36 měsíců od výrobce	kmpl	1	928 337 Kč	928 337 Kč	CON-SNT-FPR4110N
2. IPS licence							
Hardware zařízení včetně software							
1.	L-FPR4110T-T=	Cisco FPR4110 Threat Defense Threat Protection License	ks	2	0 Kč	0 Kč	L-FPR4110T-T=
2.	L-FPR4110T-T-3Y	Cisco FPR4110 Threat Defense Threat Protection 3Y Subs	ks	2	480 999 Kč	961 998 Kč	L-FPR4110T-T-3Y
Servisní podpora a prodloužení záruky od výrobce							
1.		Servisní podpora, prodloužení záruky na 36 měsíců od výrobce	kmpl	1	0 Kč	0 Kč	součást L-FPR4110T-T-3Y
3. Remote access VPN							
Hardware zařízení včetně software							
1.	L-AC-PLS-LIC=	Cisco AnyConnect Plus Term License, Total Authorized Users	ks	1000	0 Kč	0 Kč	L-AC-PLS-LIC=
2.	L-AC-PLS-3Y-S5	Cisco AnyConnect Plus License, 3YR, 1000-2499 Users	ks	1000	45 Kč	45 000 Kč	L-AC-PLS-3Y-S5
Servisní podpora a prodloužení záruky od výrobce							
1.		Servisní podpora, prodloužení záruky na 36 měsíců od výrobce	kmpl	1	0 Kč	0 Kč	součást L-AC-PLS-3Y-S5
4. Centrální management NGWF							
Hardware zařízení včetně software							
1.	FMC2600-K9	Cisco Firepower Management Center 2600 Chassis	ks	1	489 332 Kč	489 332 Kč	FMC2600-K9
2.	SF-FMC-6.3-K9	Cisco Firepower Management Center Software v6.3	ks	1	0 Kč	0 Kč	SF-FMC-6.3-K9
3.	FMC-M5-PS-AC-770W	Cisco FMC 770W AC Power Supply	ks	2	0 Kč	0 Kč	FMC-M5-PS-AC-770W
4.	FMC-M5-CPU-4110	Cisco FMC 2.1 GHz 4110 Processor, 11MB Cache, 8 Core	ks	2	0 Kč	0 Kč	FMC-M5-CPU-4110
5.	FMC-M5-MEM-16GB	Cisco FMC 16GB DDR4-2666-MHz RDIMM/PC4-21300/Single Rank	ks	4	0 Kč	0 Kč	FMC-M5-MEM-16GB
6.	FMC-M5-MRAID-12G	Cisco FMC 12G Modular RAID controller with 2GB cache	ks	1	0 Kč	0 Kč	FMC-M5-MRAID-12G
7.	FMC-M5-SD-32G	Cisco FMC 32GB SD Card Module	ks	1	0 Kč	0 Kč	FMC-M5-SD-32G
8.	FMC-M5-TPM-2.0	Cisco FMC Trusted Platform Module 2.0	ks	1	0 Kč	0 Kč	FMC-M5-TPM-2.0
9.	FMC-M5-HDD-600G	Cisco FMC 600GB 12G SAS 10K RPM SFF HDD	ks	4	0 Kč	0 Kč	FMC-M5-HDD-600G
10.	FMC-M5-MSTOR-SD	Cisco FMC Mini Storage Carrier Card for SD (holds up to 2)	ks	1	0 Kč	0 Kč	FMC-M5-MSTOR-SD
11.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	ks	2	0 Kč	0 Kč	CAB-9K10A-EU
12.	FMC-M5-NIC-SFP	Cisco FMC X710-DA2 dual-port 10G SFP+ NIC	ks	1	0 Kč	0 Kč	FMC-M5-NIC-SFP
13.	SFP-10G-SR	10GBASE-SR SFP Module	ks	2	7 917 Kč	15 834 Kč	SFP-10G-SR

Servisní podpora a prodloužení záruky od výrobce							
1.		Servisní podpora, prodloužení záruky na 36 měsíců od výrobce	kmpl	1	317 141 Kč	317 141 Kč	CON-SNT-FC2600K9
5. Implementace							
Služby							
1.	Fáze č.I	Audit a vyhotovení projektové dokumentace	MD	20	8 800 Kč	176 000 Kč	
2.	Fáze č.II	Dodávka nových hw a sw prostředků a fyzická instalace NGFW	MD	8	8 800 Kč	70 400 Kč	
3.	Fáze č.III	Přechod na nový systém NGFW	MD	24	8 800 Kč	211 200 Kč	
4.	Fáze č.IV	Optimalizace nového systému NGFW	MD	13	8 800 Kč	114 400 Kč	
Cena celkem bez DPH						**7 039 994 Kč**	

Poznámka: Pro účel zařazení majetku do evidence bude položka č. 5 - Implementace promítnuta do pořizovací ceny výše uvedených komponent dle následujícího klíče. Slouží pouze pro interní potřebu zadavatele.

Implementace položky 1. Centrální HA cluster NGFW	50%	286 000 Kč
Implementace položky 2. IPS licence	20%	114 400 Kč
Implementace položky 3. Remote access VPN	10%	57 200 Kč
Implementace položky 4. Centrální management NGWF	20%	114 400 Kč

Příloha č. 3 Kupní smlouvy č. 1309/19

SBZ03_Závazně používané standardy datových sítí

Univerzita Pardubice

Verze: 21. 11. 2017

OBSAH:

Není-li u konkrétní poptávky/zadávacího řízení z odpodstatněných důvodů požadováno jinak, platí následující obecně závazné standardy (požadavky) pro jednotlivé oblasti.

1. Strukturovaná kabeláž

1.1. Systém metalické kabeláže musí splňovat požadavky kategorie 6A, dle ISO IEC 11801 dodatek 1 (02/2008), schopného datového přenosu 10Gbit/s.

1.2. Instalovaný metalický kabel musí být schopen frekvenčního přenosu min. 1200 MHz, resp. 1500 MHz pro přenos datového, telefonního, televizního signálu, PoE a PoE+. Tato šířka pásma je určena z důvodu budoucího přechodu na vyšší přenosovou rychlost.

1.3. Instalovaný metalický kabel musí mít každý komunikační pár stíněný zvlášť pomocí kovové fólie pro odstínění rušení a indukce vysokých frekvencí a navíc musí mít kabel stínění opletením pro odstínění rušení a indukce nízkých frekvencí. Plášť musí splňovat specifikaci LSFRZH.

1.4. Všechny instalované prvky metalické kabeláže musí být ve stíněném provedení.

1.5. Instalovaný metalický kabel musí mít kategorizaci B2ca,s1,d0 dle vyhlášky 23/2008 Sb. – novelizace 268/2011 o technických podmínkách požární ochrany staveb, ze dne 29. ledna 2008 a normy EN50399, s doložením certifikátu, vydaného certifikačním orgánem, akreditovaným Českým institutem pro akreditaci.

1.6. Instalovaný optický kabel musí mít kategorizaci B2ca,s1,d1 dle vyhlášky 23/2008 Sb. – novelizace 268/2011, o technických podmínkách požární ochrany staveb, ze dne 29. ledna 2008 a normy EN50399, s doložením certifikátu vydaného certifikačním orgánem, akreditovaným Českým institutem pro akreditaci, plášť se specifikací ULSZH - nehořlavost ve svazku ISO/IEC 60332 a funkční zkouška při požáru 180 minut IEO/IEC 60331, s doložením prohlášení od výrobce (může být v českém nebo anglickém jazyce).

1.7. Nově instalovaný ucelený kabelážní systém bude realizován nejen souladu se stávající technologií, ale současně také v provedení s LED indikací portů a jeho konstrukce bude umožňovat snadný přechod na monitoring fyzické vrstvy.

1.8. Celý systém strukturované kabeláže musí splňovat podmínky pro certifikaci se systémovou garancí výrobce systému na 25 let (optická i metalická část) – Dodavatel doloží certifikát o partnerství s výrobcem systému na nejvyšší úrovni (projektování a instalace), s doložením prohlášení od výrobce (může být v českém nebo anglickém jazyce).

1.9. Instalace systému univerzální metalické i optické kabeláže musí být provedena plně v souladu s ČSN EN 50174 a se standardy a pravidly pro navrhování a montáž univerzálních kabelážních systémů. Dále musí být v souladu s požadavky vyplývajícími z Požárně bezpečnostního řešení (PBŘ) a souvisejících norem a předpisů. Celý systém včetně přípojných kabelů bude od jednoho výrobce. V datových rozvaděčích musí být ukončení metalických i optických kabelů provedeno na panelech s podporou managementu fyzické vrstvy, včetně indikace pro snadnou správu sítě.

1.10. Instalovaný systém univerzální kabeláže musí být (z provozně ekonomických důvodů – personální úspora) plně kompatibilní a odpojitelné komponenty přenositelné a zaměnitelné se stávající, již instalovanou univerzální kabeláží tak, aby např. nebylo vyžadováno:

- školení obsluhy na jiný kabelážní systém,
- tvorba jiných dokumentačních šablon (rozložení a počet portů) v elektronickém systému dokumentace,
- speciální vybavení obsluhy pro různé datové uzly, budovy, lokality

a nedocházelo:

- ke ztrátě systémové záruky při připojení komponent z jiného datového uzlu, budovy, lokality,

- k poškození komponent RJ45 při použití komponent z jiného datového uzlu, budovy, lokality,
- ke snížení zastupitelnosti osob,
- ke snížení dostupnosti služeb provozními komplikacemi.

1.11. Pokud není požadováno jinak, pro ukončení strukturované kabeláže a k instalaci aktivních prvků a záložních zdrojů v datových uzlech budou instalovány datové rozvaděče s parametry:
- min. rozměry v=2000mm, š=800mm, hl=800mm
- minimální nosnost 1300 kg
- rezerva hloubky rozvaděče musí být vpředu minimálně 50 mm a vzadu min. 100 mm, než hloubka instalovaného vybavení (z důvodu přívodu, zapojení kabeláže a proudění vzduchu)
- zamykatelné prosklené přední dveře
- přední i zadní 19“ vertikální lišty
- ventilační jednotka s termostatem do každého rozvaděče, který obsahuje aktivní prvky
- umístění kabelů datové kabeláže v rozvaděči nesmí bránit: instalaci aktivních prvků, jejich rozšiřování, výměně, správné orientaci, chlazení a používání zadních portů
- montáž aktivních prvků a záložních zdrojů UPS do rozvaděče pomocí příslušných rack-mounting kitů
- police dostatečně tuhé pro očekávané zatížení.

1.12. Při předání nainstalovaného systému strukturované kabeláže objednateli budou ze strany zhotovitele předány následující dokumenty:
- měřící protokol metalické kabeláže s uvedením naměřených hodnot měření jednotlivých portů a s doložením kalibračního protokolu použitého měřicího přístroje
- měřící protokol optické kabeláže s uvedením naměřených hodnot oboustranného měření jednotlivých vláken a s doložením kalibračního protokolu použitého měřicího přístroje
- revizní zprávu o revizi elektrického zařízení NN a uzemnění datových rozvaděčů
- montážní (stavební) deník, s uvedením všech skutečností o průběhu stavby, podepsaný zhotovitelem i objednatelem
- dokumentace skutečného stavu v papírové podobě – 2x a elektronicky na nosiči CD v upravitelné podobě 1x (výkresová část se zakreslením a popisem kabelových tras, uživatelských zásuvek a portů, technická zpráva, schéma datového rozvaděče)
- certifikát na systémovou garanci v délce 25 let od výrobce systému strukturované kabeláže. Dodání certifikátu lze odložit o 60 kalendářních dnů, což bude uvedeno jako závada v předávacím protokolu díla bez sankcí
- seznam provedených protipožárních ucpávek s doložením certifikovaného oprávnění zhotovitele, vystaveného výrobcem protipožárních ucpávek.

2. Aktivní prvky – přístupové přepínače

2.1. Obecné vlastnosti:

- L2 nebo L3 neblokující přepínače, rackmount provedení
- Minimální celková potenciální propustnost přepínacího subsystému 90 Gbit/s u 24 portového přepínače a 170 Gbit/s u 48mi portového
- Minimální celková propustnost v Mpps - 65 Mpps u 24 portového přepínače a 125 Mpps u 48mi portového
- Minimální velikost sdílených paketových bufferů na jeden přepínač - 6 MB u 24 portového přepínače a 12 MB u 48mi portového
- podpora protokolu pro definici šířených VLAN (např. VTP ve všech dostupných verzích).

- podpora záložního napájení (může být externí) , v místech, kde je nutné z hlediska redundance
- Možnost redundantního interního napájecího zdroje, vyměnitelného za chodu, v místech, kde je nutné z hlediska redundance
- IEEE 802.3, 3x (Flow Control)
- Podpora IEEE 802.3af (PoE) a IEEE 802.3at (PoE+)
- IEEE 802.1D (spanning tree)
- IEEE 802.1Q (trunking)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- podpora per VLAN rapid spanning tree – PVRST+, nebo ekvivalentní. Vyžadováno kvůli rychlejší konvergenci sítě po změně topologie či výpadku. Klasické technologie jako STP (standard 802.1D), jsou v tomto ohledu nedostačující.
- IEEE 802.3ad podpora velkých rámců (min. 9000 B)
- sdružování GB rozhraní do svazků, vyvažování přes porty ve svazku
- podpora NTP protokolu
- 10/100/1000 Gb/s pro připojení klientských stanic
- Podpora CDP protokolu, nebo obdoby umožňující identifikovat sousední zařízení na L2, např. LLDP
- Podpora UDLD protokolu dle RFC 5171 pro monitorování a detekci jednosměrných selhání / jednosměrného spoje na fyzické vrstvě – nedovoluje se použití alternativních technologií a protokolů kvůli vzájemné nekompatibilitě.
- Podpora diagnostiky připojených metalických kabelů pomocí technologie TDR
- Kombinovaná podpora uplink portů pro 1 Gbps nebo 10 Gbps
- vestavěná podpora pro úsporu energie IEEE 802.3az EEE (Energy Efficient Ethernet)
- podpora L2 raceroute (možnost snadného zjištění fyzické cesty (na L2) paketu mezi zdrojem a cílem)
- Integrovaná funkcionalita WiFi kontroleru
- Podpora distribuovaných bezdrátových vlastností (mobility) v přepínači, řízených stávajícím centrálním kontrolerem Zadavatele
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení.
- IPv6 Ready Logo fáze II – v současné době je postupný přechod k IPv6 nevyhnutelný a nelze akceptovat produkty, které na tuto změnu nejsou připraveny

2.2. Zabezpečení:

- podpora SSH v1, 2 protokolu pro vzdálenou správu přepínače
- podpora RADIUS protokolu pro AAA služby při přístupu k přepínačům
- podpora 802.1x protokolu s centralizovanou správou uživatelů na RADIUS serveru
- podpora IEEE 802.3ae v HW – L2 šifrování mezi prvky sítě. Jedná se o nutnost k zajištění zabezpečení LAN na ochranu proti útokům na druhé vrstvě (odposlouchávání, útoky typu man-in-the-middle a částečně DoS, Denial of Service) prostřednictvím průběžného monitorování, identifikace neautorizovaných stanic v LAN a zabránění související neautorizované komunikaci. Současně se chrání přenášená řídicí data šifrováním pro autentizaci zdroje dat, ochranu integrity řídicích zpráv, utajení a ochranu před přehráváním. Umožňuje plné využití 802.1× (nedílné součásti moderního zabezpečení nejen WiFi)
- podpora SNMPv3 crypto
- podpora přiřazení do VLAN z RADIUS serveru podle výsledků 802.1x autentizace
- podpora tzv. multidomain autentizace – možnost autentizace telefonu a uživatele na stejném portu a jejich správné zařazení do VLAN (telefon do VLAN pro hlas a uživatele do VLAN pro data)
- podpora RADIUS change of Authorization – možnost vynucení změny v pravidlech pro již autentizovaného uživatele/zařízení
- ochrana DHCP protokolu – blokování neautorizovaného DHCP provozu
- Inspekce ARP.
- Inspekce IP-MAC trasování.

- možnost přesměrovat data na port přepínače (pro monitorování provozu)
- podpora paketových filtrů na jednotlivých rozhraních a na terminálových spojeních na základě L2,L3,L4 informací v paketu
- možnost definovat časová omezení filtrů
- možnost omezení přístupu podle MAC adres stanic, možnost omezení maximálního počtu MAC adres za portem přepínače
- ochrana spanning tree protokolu
- Nesamplovaná metoda sběru telemetrických dat o provozu sítě/datových tocích (NetFlow). Je možné řešit také samostatnými sondami pro sběr nesamplovaného NetFlow ze všech portů poptávaného zařízení. Nedovoluje se použití technologií a protokolů, které nemonitorují veškerý datový provoz, ale pouze jeho vzorky. Hlavně v souvislosti s neustále se zvyšujícími hrozbami a četností kybernetických útoků.
- IPv6 first hop security pro zabránění útokům "man in the middle", DDoS, address spoofing – jedná se o nutný a provázaný požadavek s IPv6 certifikací a požadavky na bezpečnost

2.3. Klasifikace služeb (QoS):

- classification, policing, marking, queuing&scheduling
- IEEE 802.1p (class of service prioritization)
- podpora přednostní fronty (strict priority queueing)
- omezení toku na vstupu
- klasifikace podle DSCP

2.4. Multicast:

- podpora IGMP snooping v1,v2,v3
- podpora MLD snooping

2.5. Management:

- CLI rozhraní
- SNMPv2, SNPMv3
- TACACS+ klient
- Povyšování operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP
- Nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP
- Plná kompatibilita se stávajícím management systémem prvků LAN - Cisco Prime Infrastructure. Zařízení musí být uvedené v seznamu zde: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-device-support-tables-list.html
- Sběr parametrů o přenášených datových tocích a jejich export do nadřazených monitorovacích aplikací pomocí protokolu NetFlow Data Export verze 9 (RFC 3917, RFC 3955) nebo IPFIX. Zejména pro statistickou analýzu vytíženosti.
- Sběr parametrů o každém paketu přenášených datových toků a jejich export do nadřazených monitorovacích aplikací pomocí protokolu NetFlow Data Export verze 9 (RFC 3917, RFC 3955) nebo IPFIX. Zejména pro monitoring a zajištění bezpečnosti.
- Detailní a flexibilní definice přenášeného datového toku vyžadovaného pro sběr parametrů dle L2, L3 i L4 síťových parametrů ISO/OSI modelu.
- Sběr parametrů o přenášených datových tocích na každém portu přepínače.
- Sběr a export TCP příznaků v přenášených datových tocích pro monitoring bezpečnostních hrozeb
- Zobrazení sbíraných infromací o přenášených datových tocích přímo v přepínači. I včetně "TopN" pohledu.

- Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů přenášeného datového toku

2.6. Troubleshooting
Z důvodu snadného troubleshootingu je požadována maximální sada podporovaných nástrojů a CLI příkazů pro analýzu případných potíží

- SPAN, RSPAN, Show, Debug, Ping, Traceroute
- Logování událostí do SYSLOG serveru.
- Měření zakončení a délky metalického kabelu (TDR)
- Rozpoznání a klasifikace přenášené aplikace síťovým prvkem za spolupráce externího autoritativního serveru. Z důvodu následné aplikace požadovaných síťových/bezpečnostních/... politik na danou aplikaci. Je požadována rovněž klasifikace aplikací, které jsou přenášeny v šifrovaných spojeních.
- Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute, trasování MAC adres)
- Konfigurtovatelná interní diagnostika subsystémů a komponent zařízení. Proveditelná při startu i za běhu zařízení. Spouštitelná a využitelná správcem z příkazové řádky, plánovatelná v určitých časech a intervalech, i s návazností skriptů spouštěných přímo v zařízení po různých diagnostických výstupech.
- V zařízení zabudovaný mechanismus odchytu jednotlivých paketů pro pozdější analýzu provozu nebo analýzu v reálném čase
- Zrcadlení provozu směřujícího do centrálního procesoru (control plane) na externí analyzátor pro analýzu a řešení problémů s řídícími protokoly v síti nebo s vytížením control plane.
- Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů interpretovaných v samotném zařízení)

2.7. Automatizace

- Automatická aplikace specifické QoS konfigurace pro dané zařízení po detekci jeho připojení na portu
- Automatická aplikace specifické QoS a Security konfigurace pro dané zařízení po detekci jeho připojení na portu
- Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
- Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
- Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače
- Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů interpretovaných v samotném zařízení)
- Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury

3. Aktivní prvky - distribuční přepínače

3.1. Obecné vlastnosti:

- L3 neblokující přepínače, rackmount provedení
- Minimální celková potenciální propustnost přepínacího subsystému 750 Gbit/s
- Minimální celková propustnost centrálních řídících modulů (IPv4/IPv6) - 245/120 Mpps
- Minimální velikost sdílených paketových bufferů 32 MB na jeden přepínač
- podpora OSPF
- podpora OSPF s MD5 a NSSA
- podpora RIPv2
- podpora Policy-based routing podle ACL

- podpora Statické směrování
- podpora EIGRP stub routing (dle RFC draft-savage-eigrp-01)
- podpora protokolu pro definici šířených VLAN (např. VTP ve všech dostupných verzích).
- podpora záložního napájení (může být externí) , v místech, kde je nutné z hlediska redundance
- Možnost redundantního interního napájecího zdroje, vyměnitelného za chodu, v místech, kde je nutné z hlediska redundance
- IEEE 802.3, 3x (Flow Control)
- IEEE 802.1D (spanning tree)
- IEEE 802.1Q (trunking)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- podpora per VLAN rapid spanning tree – PVRST+, nebo ekvivalentní. Vyžadováno kvůli rychlejší konvergenci sítě po změně topologie či výpadku. Klasické technologie jako STP (standard 802.1D), jsou v tomto ohledu nedostačující.
- IEEE 802.3ad podpora velkých rámců (min. 9000 B)
- sdružování GB a 10GB rozhraní do svazků, vyvažování přes porty ve svazku
- podpora NTP protokolu
- 1 a 10 Gb/s pro připojení přístupových přepínačů
- Podpora CDP protokolu, nebo obdoby umožňující identifikovat sousední zařízení na L2, např. LLDP
- Podpora UDLD protokolu dle RFC 5171 pro monitorování a detekci jednosměrných selhání / jednosměrného spoje na fyzické vrstvě – nedovoluje se použití alternativních technologií a protokolů kvůli vzájemné nekompatibilitě.
- Kombinovaná podpora portů pro 1 Gbps nebo 10 Gbps
- podpora L2 raceroute (možnost snadného zjištění fyzické cesty (na L2) paketu mezi zdrojem a cílem)
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení.
- IPv6 Ready Logo fáze II – v současné době je postupný přechod k IPv6 nevyhnutelný a nelze akceptovat produkty, které na tuto změnu nejsou připraveny
- Podpora HSRP nebo VRRP pro IPv6
- Podpora IPv6 ACL
- Podpora IPv6 QoS
- Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP).

3.2. Zabezpečení:

- podpora SSH v1, 2 protokolu pro vzdálenou správu přepínače
- podpora RADIUS protokolu pro AAA služby při přístupu k přepínačům
- podpora 802.1x protokolu s centralizovanou správou uživatelů na RADIUS serveru
- podpora IEEE 802.3ae v HW – L2 šifrování mezi prvky sítě. Jedná se o nutnost k zajištění zabezpečení LAN na ochranu proti útokům na druhé vrstvě (odposlouchávání, útoky typu man-in-the-middle a částečně DoS, Denial of Service) prostřednictvím průběžného monitorování, identifikace neautorizovaných stanic v LAN a zabránění související neautorizované komunikaci. Současně se chrání přenášená řídicí data šifrováním pro autentizaci zdroje dat, ochranu integrity řídicích zpráv, utajení a ochranu před přehráváním. Umožňuje plné využití 802.1× (nedílné součásti moderního zabezpečení nejen WiFi)
- podpora SNMPv3 crypto
- podpora RADIUS change of Authorization – možnost vynucení změny v pravidlech pro již autentizovaného uživatele/zařízení
- ochrana DHCP protokolu – blokování neautorizovaného DHCP provozu
- Inspekce ARP.
- Inspekce IP-MAC trasování.
- možnost přesměrovat data na port přepínače (pro monitorování provozu)

- podpora paketových filtrů na jednotlivých rozhraních a na terminálových spojeních na základě L2,L3,L4 informací v paketu
- možnost definovat časová omezení filtrů
- možnost omezení přístupu podle MAC adres stanic, možnost omezení maximálního počtu MAC adres za portem přepínače
- ochrana spanning tree protokolu
- Nesamplovaná metoda sběru telemetrických dat o provozu sítě/datových tocích (NetFlow). Je možné řešit také samostatnými sondami pro sběr nesamplovaného NetFlow ze všech portů poptávaného zařízení. Nedovoluje se použití technologií a protokolů, které nemonitorují veškerý datový provoz, ale pouze jeho vzorky. Hlavně v souvislosti s neustále se zvyšujícími hrozbami a četností kybernetických útoků.
- IPv6 first hop security pro zabránění útokům "man in the middle", DDoS, address spoofing – jedná se o nutný a provázaný požadavek s IPv6 certifikací a požadavky na bezpečnost.

3.3. Klasifikace služeb (QoS):

- classification, policing, marking, queuing&scheduling
- IEEE 802.1p (class of service prioritization)
- podpora přednostní fronty (strict priority queueing)
- omezení toku na vstupu
- klasifikace podle DSCP.

3.4. Multicast:

- podpora IGMP snooping v1,v2,v3
- podpora MLD snooping
- podpora IPv6 Multicast (MLDv1 & v2)
- podpora IPv6 Multicast (PIM SSM)
- podpora IPv6 Multicast (PIM SM)
- podpora PIM (dense i sparse mód)
- podpora Source-Specific Multicast (SSM)
- podpora IGMPv2
- podpora IGMPv3
- podpora IPv6 MLDv1 & v2 snooping.

3.5. Management:

- CLI rozhraní
- SNMPv2, SNPMv3
- TACACS+ klient
- Povyšování operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP
- Nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP
- Plná kompatibilita se stávajícím management systémem prvků LAN - Cisco Prime Infrastructure. Zařízení musí být uvedené v seznamu zde: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-device-support-tables-list.html
- Sběr parametrů o přenášených datových tocích a jejich export do nadřazených monitorovacích aplikací pomocí protokolu NetFlow Data Export verze 9 (RFC 3917, RFC 3955) nebo IPFIX. Zejména pro statistickou analýzu vytíženosti.
- Sběr parametrů o každém paketu přenášených datových toků a jejich export do nadřazených monitorovacích aplikací pomocí protokolu NetFlow Data Export verze 9 (RFC 3917, RFC 3955) nebo IPFIX. Zejména pro monitoring a zajištění bezpečnosti.
- Detailní a flexibilní definice přenášeného datového toku vyžadovaného pro sběr parametrů dle L2, L3 i L4 síťových parametrů ISO/OSI modelu.
- Sběr parametrů o přenášených datových tocích na každém portu přepínače.

- Sběr a export TCP příznaků v přenášených datových tocích pro monitoring bezpečnostních hrozeb
- Zobrazení sbíraných infromací o přenášených datových tocích přímo v přepínači. I včetně "TopN" pohledu.
- Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů přenášeného datového toku.

3.6. Troubleshooting

Z důvodu snadného troubleshootingu je požadována maximální sada podporovaných nástrojů a CLI příkazů pro analýzu případných potíží

- SPAN, RSPAN, Show, Debug, Ping, Traceroute
- Logování událostí do SYSLOG serveru.
- Rozpoznání a klasifikace přenášené aplikace síťovým prvkem za spolupráce externího autoritativního serveru. Z důvodu následné aplikace požadovaných síťových/bezpečnostních/... politik na danou aplikaci. Je požadována rovněž klasifikace aplikací, které jsou přenášeny v šifrovaných spojeních.
- Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute, trasování MAC adres)
- Konfigurtovatelná interní diagnostika subsystémů a komponent zařízení. Proveditelná při startu i za běhu zařízení. Spouštitelná a využitelná správcem z příkazové řádky, plánovatelná v určitých časech a intervalech, i s návazností skriptů spouštěných přímo v zařízení po různých diagnostických výstupech.
- V zařízení zabudovaný mechanismus odchytu jednotlivých paketů pro pozdější analýzu provozu nebo analýzu v reálném čase
- Zrcadlení provozu směřujícího do centrálního procesoru (control plane) na externí analyzátor pro analýzu a řešení problémů s řídícími protokoly v síti nebo s vytížením control plane.
- Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů interpretovaných v samotném zařízení).

3.7. Automatizace

- Automatická aplikace specifické QoS konfigurace pro dané zařízení po detekci jeho připojení na portu
- Automatická aplikace specifické QoS a Security konfigurace pro dané zařízení po detekci jeho připojení na portu
- Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
- Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
- Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače
- Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů interpretovaných v samotném zařízení)
- Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury.

4. Aktivní prvky - bezdrátové zařízení (access pointy)

4.1. Obecné vlastnosti:

- podporují přenosové rychlosti dle specifikací norem IEEE 802.11a,b,g,n, ac (wave 2)
- napájení přímo po ethernetovém kabelu pomocí Power-Over-Ethernet+ (PoE+) – jsou nepřípustná zařízení používající Pasivní PoE (tj. nekompatibilní s normou IEEE 802.3af či taková, která potřebují speciální adaptér)
- uzamykatelná montážní konzole
- podpora simultánního vícepásmového provozu
- optimalizace a formování více signálů pro jednoho klienta
- podpora 160 MHz kanálů
- pro vybrané modely - možnost rozšíření o externí moduly
- autentizace – 802.1X (LEAP, EAP-FAST, PEAP-GTC, PEAP-Microsoft, PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, EAP-SIM, MAC adres autentizace
- šifrování - AES-CCMP encryption (WPA2),
- podpora pro šifrování AES v HW
- podpora IEEE 802.11i
- ethernetové rozhraní 802.3bz (mGig = podpora multigigabit ethernetu – možnost volby rychlosti portu 100Mbps,1, 2.5 a 5 Gbps přes standardní metalickou kabeláž normy 5e)
- podpora managementu prostřednictvím SSH, HTTPS, SNMP
- podpora VLAN, mapování VLAN na SSID
- podpora minimálně 4x4 MIMO a 3 spatial streamů
- podpora automatické analýzy rádiového spektra s možností automatického přeladění AP na jiný nezarušený (či méně zarušený) kanál
- podpora Dual 5 GHz rádia
- možnost automatického povolení 802.11r na WLAN SSID bez omezení možnosti připojení pro non 802.11r zařízení (integrace s Apple zařízeními)
- Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP, možnost selektivního využití 802.11r na sdíleném SSID pouze pro Apple zařízení, které tento standard podporují
- možnost upřednostnění aplikačního provozu (podpora QoS) od mobilního iOS10 a novějšího klienta směrem k bezdrátovému prvku – video, voice – zlepšení uživatelské skušenosti s aplikacemi pro telekonferenční hovory, stream videa apod.
- možnost umístnění kontroleru na každý pořizovaný přístupový bod s podporou 802.11 ac Wave 2 – ochrana investice v případě nutnosti změny sítě
- komplementarita s nadstavbovým analytickým nástrojem umožňujícím lokalizaci klientů
- podpora IEEE 802.1Q na fyzickém Ethernet portu
- podpora komunikace s centrálním prvkem přes standardizovaný protokol CAPWAP (RFC 5416)
- Možnost omezení přístupu k managementu
- možnost integrace se stávajícím centrálním managementem bezdrátové sítě na úrovni řízení WiFi AP ze stávajícího centrálního kontroleru Zadavatele
- Plná kompatibilita se stávajícím management systémem prvků LAN - Cisco Prime Infrastructure. Zařízení musí být uvedené v seznamu zde: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-device-support-tables-list.html

5. Požadavky na záruku a technickou podporu všech typů aktivních prvků výše uvedených

- Dodavatel poskytne Zadavateli po dobu trvání podpory všechny relevantní SW releases a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad. Dodavatel 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. Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.

- Dodavatel je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízení tak, aby v případě závady na dodaných zařízeních, kterou není Dodavatel schopen sám odstranit, bylo možné tuto závadu eskalovat přímo k výrobci zařízení. Zároveň je Dodavatel povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- Dodavatel je povinen zajistit dostupnost náhradních dílů od výrobce a dostupnost vlastní podpory pro dodané řešení za podmínek specifikovaných Zadavatelem.
- Výše specifikovanou podporu a dostupnost náhradních dílů Zadavatel požaduje po dobu min. 5 let od data dodání.
- Dodavatel zajistí seznámení zástupců Zadavatele a jejich proškolení pro práci s nástroji pro centrální správu, s funkcemi administrátorského přístupu k nástrojům jednotlivých funkcí, se zabezpečeným přístupem pro vzdálenou správu jednotlivých komponent (https, ssh), s grafickým rozhraním pro správu jednotlivých komponent řešení, s nástroji pro hromadné a dávkové konfigurace a s nástroji pro monitorování technických parametrů systému.
- Všechna dodaná síťová zařízení musí pocházet od stejného výrobce a musí být 100% kompatibilní se zařízením používaným v současné době.
- Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení) pro český trh a koncového Zákazníka - Zadavatele, pokud o to Zadavatel požádá. Zadavatel požaduje originální a nové zařízení, licencované na jméno Zákazníka tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
- Výrobce nabízených aktivních síťových prvků má implementován tzv. “SDL - secure development lifecycle “ při vývoji svých produktů a tzv. “SIRT - Security Incident Response Team” pro reportování bezpečnostních incidentů spojených s nabízenými produkty.
- Musí být možno se zaregistrovat na stránkách výrobce (na přímém internetovém odkazu) k odběru automatických mailových zpráv týkajících se zařízení a upozorňujících s denní frekvencí na:
    1. bezpečnostní incidenty, které vyžadují od Zadavatele povýšení operačního systému/firmware či aplikování změny konfigurace či záplaty,
    2. konec prodeje či podpory,
    3. nové verze operačního systému/firmware
    4. známé chyby operačního systému/firmware.
- Musí být možno v rámci záruky instalovat obraz virtuálního serveru výrobce, který bude plnit funkci sondy a bude zajišťovat automaticky funkce uvedené v předchozím odstavci bez nutnosti zpřístupnit zařízení mimo zabezpečenou část sítě.

6. Záložní zdroje napájení

6.1. Obecné vlastnosti:

- dvojkonverzní on-line záložní zdroj
- nulový čas přepnutí na baterie
- široký rozsah vstupního napětí 160-280V
- sinusový výstup
- korekce vstupního účiníku
- automatický bypass
- škálovatelnost doby běhu přidáváním externích baterií
- definici výstupního napětí (220/230/240)
- programování výstupní frekvence
- rackové provedení, UPS obsahuje odpovídající příslušenství pro montáž do racku

- snadno vyměnitelné baterie za provozu
- minimální doba běhu všech připojených zařízení na baterie 15 minut
- studený start (možnost zapnutí záložního zdroje i při úplném výpadku napájecího proudu)
- u UPS se jmenovitým výkonem 10kVA a vyšším, možnost odpojení/přemostění UPS pomocí manuálního BY-PASSu.
- UPS obsahuje rozhraní RJ45, pro vzdálený monitoring po síti LAN, nebo interní zásuvný modul s rozhraním RJ45 pro vzdálený monitoring po síti LAN.
- interní zásuvný modul UPS musí být (z provozně ekonomických důvodů) plně kompatibilní, přenositelný a zaměnitelný s ostatními stávajícími, již instalovanými interními zásuvnými moduly v jiných UPS.
- Jednotný dohled a správa záložních zdrojů.

6.2. Motorgenerátor

- připojení do datové sítě pro možnost sledování běhu motorgenerátoru
- management přes Web/SNMP (rozhraní RJ 45 10/100BaseT a sériový komunikační port).

7. Standardy architektury

Bývají konkretizovány projektem pro každou zakázku, jestliže ne, platí požadovaný stav:

- hlavní přepínač řešené budovy bude propojen optickou linkou o rychlosti 10 Gb/s do (jednoho nebo i druhého) datového centra Zadavatele
- ostatní přepínače budou připojeny k páteřnímu přepínači rychlostí 10Gbps nebo 1 Gb/s
- koncoví uživatelé budou do datové sítě připojeni rychlostí 1 Gb/s
- celá dodávka nových aktivních prvků musí být tvořena zařízeními od jednoho výrobce a musí být zajištěna plná funkcionalita se stávající počítačovou sítí. Výjimku můžou tvořit zdroje záložního napájení, které mohou být od jiného výrobce.
- vícezdrojové přepínače budou zálohovány dvěma záložními zdroji napětí a to vždy jeden zdroj aktivního prvku (přepínače) na jeden záložní zdroj.
- V každém řešeném datovém uzlu musí být minimálně jeden modul nebo přepínač se 48 porty UTP, které mají funkcionalitu Power over Ethernet+ (PoE+).
- Páteřní připojení datového uzlu k nadřazenému datovému centru/uzlu musí zahrnovat minimálně tyto kabely:
  - Připojení optickým kabelem singlemode min. 8 vláken
  - Připojení telefonním kabelem CAT3 min. 10 párů.

8. Standardy datového uzlu nebo centra

Datový uzel: obsahuje komponenty pro provoz budovy, nebo její části - rozvaděče, zakončení pasivní kabeláže, aktivní prvky, UPS, případně dalších systémů např. AV techniky, CCTV, EPS, EZS, ...

- minimální šířka přístupu (dveří): 900 mm
- čtečka u dveří napojená na centrální přístupový systém
- dveřní kontakt a prostorové čidlo napojené na centrální EZS
- protipožární čidlo napojené na centrální EPS
- klimatizace prostoru (do celkového příkonu 5 kW 1 klimatizační jednotka, jinak 2 nezávislé klimatizační jednotky), funkce autostart (automatický náběh po výpadku napájení)
- samostatný elektro rozvaděč s jištěnými okruhy a měřením spotřeby energie
- v místnosti nejsou rozvody vody ani odpady
- 2 patra nad místností není provozován vodovod ani WC.

Datové centrum: obsahuje komponenty pro připojení datových uzlů a provoz centralizovaných služeb. Proti datovému uzlu obsahuje více spotřebičů, servery, datová úložiště apod.

- Všechny výše uvedené parametry platné pro datové uzly a dále:
- nosnost podlahy (stavbou nebo statickým posudkem) deklarovaná min 800 kg/m2
- bezpečnostní dveře
- napájení instalovaných zařízení přes motorgenerátor
- antistatická podlaha
- rozvaděče pro servery:
  - hloubka 1200 mm
  - přední dveře jednodílné, děrované
  - zadní dveře dvoudílné, děrované
  - nosnost min. 1300 kg.

9. Standardy servisní smlouvy / záruky

9.1. Odstranění závady

Minimální požadavky na odstranění závady u aktivních prvků.
Kategorie:

- „A“ – odstranění závady do 4 hodin, aktivní prvky
- „B“ – odstranění závady do 12 hodin, vše ostatní
- „C“ – odstranění závady do 48 hodin, vše ostatní.

9.2. Záruka/servis aktivní prvky

Požadavky na dodávané aktivní prvky.

- záruka na hw na 4 roky
- řešení reklamace do 5 pracovních dní
- při reklamačním procesu zůstává vadné zboží u Zákazníka
- bezplatný přístup k novým verzím firmware po dobu 3 roků
- řešení složitějších technických problémů v češtině pomocí lokálního partnera výrobce aktivních prvků.

9.3. Záruka záložní zdroje

- záruka na hw 4 roky

10. Jazykové verze

Veškeré dokumentace vztahující se k Zadavateli, konzultace, jednání a servisní podpora jsou vyžadovány v češtině. Ostatní dokumentace, manuály a produktové listy jsou vyžadovány v angličtině nebo češtině.