KUPNÍ SMLOUVA O DODÁVCE SYSTÉMU MONITORINGU A SÍŤOVÉ SPRÁVY

Lesy České republiky, s.p.
se sídlem: Přemyslova 1106/19, Nový Hradec Králové, 500 08 Hradec Králové
IČO: 42196451
DIČ: CZ42196451
[redacted]
zastoupený Ing. Danielem Szórádem, Ph. D., generálním ředitelem
zapsaný v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, oddíl AXII, vložka 540

dále jen „**kupující**"

a

Huatech a.s.
se sídlem: Vyskočilova 741/3, Michle, 140 00 Praha 4
IČO: 03665496
DIČ: CZ03665496
[redacted]
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 20333
zastoupená Ing. Martinem Vítkem, jediným členem představenstva

dále jen „**prodávající**"

uzavírají v souladu s § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**občanský zákoník**"), níže uvedeného dne, měsíce a roku tuto

kupní smlouvu o dodávce systému monitoringu a síťové správy
(dále jen „**Smlouva**" nebo též „**KS**")

1. Úvodní ustanovení

1.1. Smlouva je smlouvou na plnění veřejné zakázky zadané v rámci dynamického nákupního systému s názvem „Dodávky výpočetní a kancelářské techniky a příslušenství II", jehož zavedení bylo oznámeno uveřejněním otevřeného řízení ve Věstníku veřejných zakázek pod ev. č. Z2017-007417dále jen „**DNS**").

1.2. Smlouva je uzavřena na základě výsledků řízení k zadání veřejné zakázky v DNS „Výzva k podání nabídek č. 2 – Řízení přístupů do podnikové sítě a bezpečnostní monitoring datového provozu" v DNS zahájeného výzvou k podání nabídky ve smyslu § 141 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**"), odeslanou dne 11. 9. 2017 a v souladu s nabídkou Prodávajícího podanou v tomto zadávacím řízení.

2. Předmět koupě

2.1. Předmětem Smlouvy je závazek prodávajícího dodat kupujícímu systém pro monitoring a správu sítě ve formě software a hardware, blíže specifikované v příloze č. 1 této Smlouvy – Technické specifikaci, v požadovaném celkovém počtu dle cenové nabídky, která je součástí přílohy č. 2 této Smlouvy – Ceniku (dále jen „předmět koupě"), a to včetně zajištění jejich dodávky do místa plnění, instalace a implementace, školení, dodávky software, jeho nových verzí a updatů, jakož i poskytnout kupujícímu další související plnění, a to v rozsahu a za podmínek stanovených touto Smlouvou. Kupující se zavazuje řádně dodané plnění převzít a zaplatit za ně, jakož i za ostatní dle této Smlouvy řádně poskytnutá plnění dohodnutou kupní cenu.

2.2. Kupující se zavazuje poskytnout veškerou součinnost nezbytnou pro dodání předmětu koupě a jeho instalaci, a po jeho převzetí, stvrzeném podpisy předávacího protokolu oprávněnými zástupci obou smluvních stran, uhradit kupní cenu dle čl. 4. této Smlouvy.

2.3. Pokud je součástí dodávaného hardware i obslužný software, musí být plně funkční a dodán v rozsahu nezbytném pro maximální využití dodávaného hardware, a to vše včetně veškerých úrovní přístupů do jednotlivých prvků předmětu koupě.

3. Dodací podmínky

3.1. Prodávající se zavazuje dodat kupujícímu předmět koupě uvedený v čl. 2. této Smlouvy dle harmonogramu uvedeného v Příloze č. 4 této Smlouvy.

3.2. Místem plnění pro jednotlivé typy dodaných komponent systémů pro monitoring a správu sítě jsou následující adresy:

Sídlo zadavatele: Přemyslova 1106/19, 500 08 Hradec Králové
Krajská ředitelství:

Brandýs nad Labem	Nábřeží 120, Brandýs nad Labem, 250 01
Brno	Jezuitská 13, Brno, 602 00
České Budějovice	Sadová 2388/19, Dobrá Voda u Českých Budějovic, 373 16
Frýdek-Místek	Nádražní 2811, Frýdek-Místek, 738 01
Choceň	Za drahou 191, Týniště nad Orlicí
Jihlava	Lidická kolonie 39, Jihlava, 586 01
Karlovy Vary	Krušnohorská 7, Karlovy Vary, 360 10
Liberec	Sokolská 1383, Liberec 1, 460 01
Plzeň	Sukova 40, Plzeň, 301 00
Šumperk	Potoční 22, Šumperk, 787 01
Teplice	Dr. Vrbenského 2874/1, Teplice, 415 01
Zlín	Březnická 5659, Zlín, 760 01

3.3. Prodávající dohodne s kupujícím termín předání předmětu koupě pro každé z míst plnění nejméně 5 dní předem, aby byl kupující schopen poskytnout mu potřebnou součinnost.

3.4. Prodávající je povinen dodat předmět koupě v pracovní době kupujícího. Nebude-li v konkrétním případě smluvními stranami dohodnuto jinak je v pracovní dny možné předmět koupě dodat v době od 8:00 do 16:00 hod.

3.5. O předání a převzetí předmětu koupě pro každé z míst plnění bude pořízen předávací protokol obsahující výčet a počty kusů dodaného hardware, vč. sériových čísel prvků. Předávací protokol bude datován a podepsán oprávněnými zástupci obou smluvních stran.

3.6. Kupující nabývá vlastnického práva k předmětu koupě jeho řádným předáním; týmž okamžikem přechází na kupujícího nebezpečí škody na předmětu koupě, popř. jeho části.

4. Kupní cena

4.1. Kupující se zavazuje zaplatit prodávajícímu za řádně poskytnutá plnění dle této Smlouvy kupní cenu ve výši stanovené v cenové nabídce, která je součástí přílohy č. 2 této Smlouvy – Ceníku; cenová nabídka obsahuje též položkové členění kupní ceny. Ke kupní ceně bude připočtena DPH ve výši dle příslušných právních předpisů.

4.2. Kupní cena je cenou konečnou, nejvýše přípustnou a nemůže být měněna, přičemž současně zahrnuje veškeré náklady spojené s plněním Smlouvy – zejména dodávkou předmětu koupě kupujícímu (jako např. balné, náklady na dopravu do místa plnění, náklady na pojištění během dopravy, instalaci (zahrnující zejména hardware instalaci, kompletní zprovoznění a oživení, apod.) a zajištěním servisu. Prodávající tak není v souvislosti s plněním Smlouvy oprávněn účtovat a požadovat na Kupujícím úhradu jakýchkoliv jiných či dalších částek.

5. Platební podmínky

5.1. Úhrada kupní ceny bude kupujícím provedena na základě faktury – daňového dokladu řádně vystaveného prodávajícím po předání každého uceleného dílčího předmětu koupě pro každé z míst plnění stvrzeného podpisem předávacího protokolu oprávněnými zástupci obou smluvních stran.

5.2. Lhůta splatnosti faktury – řádně vystaveného daňového dokladu – byla dohodnuta na 21 kalendářních dnů ode dne jeho doručení kupujícímu.

5.3. Faktura musí obsahovat veškeré náležitosti daňového dokladu stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Přílohou faktury bude kopie předávacího protokolu s náležitostmi dle čl. 3. odst. 3.5 této Smlouvy, stvrzujícího předání předmětu koupě, za nějž je účtováno. V případě, že faktura nebude obsahovat některou z předepsaných náležitostí či některý požadavek stanovený Smlouvou, nelze takovouto fakturu považovat za řádně vystavenou a Kupující je oprávněn vrátit ji Prodávajícímu bez proplacení zpět, a to aniž by se dostal do prodlení s úhradou kupní ceny. Lhůta splatnosti v takovém případě neběží, přičemž nová lhůta splatnosti počíná běžet až od doručení opravené či doplněné faktury (včetně požadovaných příloh).

5.4. Kupující nebude poskytovat jakékoliv zálohy na kupní cenu.

5.5. Veškeré cenové údaje podle Smlouvy musí být uvedeny v českých korunách a veškeré platby podle Smlouvy budou prováděny v české měně. Za den uskutečnění zdanitelného plnění je považován den podpisu předávacího protokolu oběma smluvními stranami.

5.6. Fakturační adresou je adresa sídla kupujícího.

5.7. Stane-li se prodávající nespolehlivým plátcem ve smyslu § 106a zák. č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (zákon o DPH), je povinen neprodleně o tomto písemně informovat kupujícího.

5.8. Bude-li prodávající ke dni poskytnutí zdanitelného plnění veden jako nespolehlivý plátce ve smyslu § 106a zákona o DPH, je kupující oprávněn část ceny odpovídající dani z přidané hodnoty uhradit přímo na účet správce daně v souladu s ust. § 109a zákona o DPH. Prodávající obdrží pouze cenu předmětu koupě bez DPH.

6. Záruka za jakost a odpovědnost za vady

6.1. Prodávající poskytuje na předmět koupě záruku za jakost ve smyslu § 2113 a násl. občanského zákoníku o době trvání 2 let. Záruka je poskytována v režimu hlášení závad 8 hodin denně, 5 pracovních dní v týdnu, s výměnou vadného dílu dle postupu blíže specifikovaného v odst. 6.3 a čl. 7 Smlouvy, tj. v režimu NBD. Dodavatel je dále povinen doložit doklad o zaplacení technické podpory přímo u výrobce nebo servisního partnera výrobce daného předmětu dodávky.

Záruční doba počíná běžet dnem řádného dodání a převzetí předmětu koupě kupujícím dle čl. 3.5. této Smlouvy.

6.2. Vady je kupující povinen oznámit (reklamovat) prodávajícímu prostřednictvím faxové zprávy či elektronické pošty (e-mailem) na adrese prodávajícího nebo hlášením na servisní linku prodávajícího **support@huatech.cz, +420 840 11 22 33**. Prodávající potvrdí kupujícímu obratem, nejpozději však do 4 hodin od okamžiku nahlášení vady (v souladu s druhým odstavcem bodu 7.1. této Smlouvy), přijetí reklamace e-mailem na adresu ServisIT@lesycr.cz. Oznámení musí obsahovat stručný popis toho, v čem je vada předmětu koupě spatřována. Současně s oznámením vady sdělí kupující prodávajícímu nárok z vad (způsob vyřízení reklamace), který si kupující zvolil v souladu s § 2106 a § 2107 občanského zákoníku.

6.3. V případě, že kupující oznámí prodávajícímu vadu předmětu koupě, zavazuje se prodávající po celou záruční dobu dle odst. 6.1. tohoto článku Smlouvy vyřídit reklamaci a bezplatně odstranit vady a zprovoznit předmět koupě v místě dodání a instalace a to nejpozději do konce následujícího pracovního dne po nahlášení vady kupujícím (služba NBD blíže specifikovaná v čl. 7 Smlouvy), pokud se smluvní strany písemně nedohodnou jinak. Po dobu trvání záruky zajistí prodávající přístup k nejnovějším verzím programového vybavení.

6.4. Na základě oznámení vad je prodávající povinen vydat kupujícímu potvrzení o tom, kdy byly vady prodávajícímu oznámeny, v čem kupující vady spatřuje a jaký způsob vyřízení reklamace kupující požaduje. Po vyřízení reklamace je prodávající povinen vydat kupujícímu potvrzení o datu a způsobu vyřízení reklamace (zejména dokladující provedení opravy, dobu jejího trvání, popř. písemné odůvodnění zamítnutí reklamace).

6.5. V případě oprávněné reklamace je prodávající povinen nahradit kupujícímu veškeré náklady, které kupující účelně vynaložil v souvislosti s uplatněním nároku z vad předmět koupě. Náhradu těchto nákladů poskytne prodávající na základě písemné výzvy kupujícího doručené prodávajícímu. Náhrada nákladů je splatná do 21 dnů ode dne doručení výzvy podle předchozí věty.

6.6. Prodávající prohlašuje, že výrobce/výrobci jednotlivých částí předmětu koupě mají servisního partnera v České republice.

Adresa a kontakt na autorizované servisy výrobce v České republice:

- Flowmon networks komponenty řešení:
  - Huatech a.s. – Vyskočilova 741/3, Praha 4 (IČO: 03665496)
  - Flowmon Networks a.s. - - Sochorova 3232/34, Žabovřesky, 616 00 Brno (IČO: 27730450)
- Novicom komponenty řešení:
  - Huatech a.s. – Vyskočilova 741/3, Praha 4 (IČO: 03665496)
  - Novicom, s.r.o. – Ořech, Husí Plácek 192, PSČ 25225 (IČO: 61465445)

7. Servisní služby, technické podpora

7.1. Prodávající se zavazuje poskytovat kupujícímu ve vztahu k předmětu koupě po celou záruční dobu dle čl. 6 odst. 6.1 Smlouvy bezplatnou servisní podporu (službu) NBD v rozsahu minimálně 8 hodin denně (v rozmezí od 8:00 do 16:00 hod.), 5 pracovních dní v týdnu s tím, že případné vady předmětu koupě budou po dobu trvání záruky za jakost bezplatně odstraněny a hardware zprovozněn v místě instalace předmětu koupě nejpozději do konce následujícího pracovního dne po nahlášení vady kupujícím.

V případě, že vada bude kupujícím oznámena prodávajícímu mimo dobu poskytované služby NBD, považuje se za okamžik nahlášení vady nejbližší okamžik zahájení poskytování služby NBD.

7.2. Prodávající zajistí emailovou a webovou hotline podporu, dostupnou 24 hodin denně 7 dní v týdnu. Servisní technická podpora bude dostupná v českém jazyce.

8. Požadavky na realizační tým prodávajícího

8.1. Prodávající se zavazuje v rámci projektu zajistit realizaci osobami s potřebnou specializací a odbornou kvalifikací, v rolích uvedených v odst. 8.3 až 8.5.

8.2. Prodávající se zavazuje, že osoby uvedené v seznamu členů odborného týmu v rámci přílohy č. 3 Smlouvy se budou fakticky přímo podílet na realizaci této smlouvy, a to ve vztahu k požadovaným pozicím, resp. v rozsahu odpovídajícím požadovaným zkušenostem a potřebám při plnění této smlouvy.

8.3. Specialista pro roli Projektový manažer musí dále splňovat následující podmínky:

- má dokončené VŠ vzdělání technického či ekonomického směru v oboru informačních a komunikačních technologií;
- má certifikaci pro oblast projektového řízení – minimálně na úrovni IPMA D nebo PRINCE2 INTRO nebo ekvivalentní, či vyšší;
- má certifikaci pro oblast ITSM (IT service management) – minimálně na úrovni ITIL v3 Foundation nebo ekvivalentní, či vyšší;
- má praxi v oblasti ICT minimálně 5 let;

- podílel se v roli Projektového manažera na minimálně třech projektech, jejichž předmětem byla implementace minimálně obdobného rozsahu ICT technologií, přičemž finanční hodnota každého z projektů činila minimálně 2.000.000 Kč bez DPH.

8.4. **Specialista pro roli Senior technik musí dále splňovat následující podmínky:**

- má dokončené VŠ vzdělání technického či ekonomického směru v oboru informačních a komunikačních technologií;
- má praxi v oblasti ICT minimálně 5 let;
- má platnou certifikaci od výrobce dodávané technologie minimálně na úrovni Technical Specialist - Network Performace Monitoring and Diagnostics;
- má platnou certifikaci od výrobce dodávané technologie minimálně na úrovni technického specialisty v oblasti bezpečnosti Technical Specialist - Security, či obdobnou nebo vyšší;
- má certifikaci od výrobce síťových technologií Huawei Technologies minimálně na úrovni Huawei Certified Network Professional - Routing and Switching, nebo vyšší;
- podílel se v roli Senior technika na minimálně dvou projektech, jejichž předmětem byla implementace minimálně obdobného rozsahu ICT technologií, přičemž finanční hodnota každého z projektů činila nejméně 2.000.000 Kč bez DPH.

8.5. **Specialista pro roli Junior technik musí dále splňovat následující podmínky:**

- má dokončené VŠ vzdělání technického či ekonomického směru v oboru informačních a komunikačních technologií;
- má praxi v oblasti ICT minimálně 2 roky;
- má platnou certifikaci od výrobce dodávané technologie minimálně na úrovni Network Consultant, či obdobnou, nebo vyšší;
- má certifikaci od výrobce síťových technologií Huawei Technologies minimálně na úrovni Huawei Certified Network Professional - Routing and Switching, nebo vyšší;
- podílel se v roli Junior technika na minimálně dvou projektech, jejichž předmětem byla implementace minimálně obdobného rozsahu ICT technologií, přičemž finanční hodnota každého z projektů činila nejméně 2.000.000,- Kč bez DPH.

8.6. Prodávající je oprávněn specialisty uvedené v seznamu členů odborného týmu jednostranně změnit, a to prostřednictvím písemného oznámení doručeného druhé smluvní straně. Společně s takovým oznámením doloží prodávající kupujícímu, doklady prokazující splnění podmínek požadovaných pro konkrétní roli novým specialistou. Změna je účinná okamžikem doručení oznámení druhé smluvní straně.

9. Odpovědnost za škodu

9.1. Prodávající odpovídá za veškerou škodu vzniklou kupujícímu nebo třetím osobám v souvislosti s plněním, nedodržením nebo porušením jakékoliv povinnosti prodávajícího vyplývající ze Smlouvy.

9.2. Odpovědnost za škodu se řídí § 2894 a násl. občanského zákoníku.

9.3. Prodávající není oprávněn požadovat náhradu škody vzniklé v důsledku prodlení kupujícího s úhradou kupní ceny.

10. Smluvní pokuty

10.1. V případě prodlení prodávajícího s řádným dodáním a instalací předmětu koupě oproti termínu sjednanému v odst. 3.1. této Smlouvy zavazuje se prodávající zaplatit kupujícímu smluvní pokutu ve výši 2.000,- Kč za každý, byť i jen započatý, den prodlení. Uplatněním práva na smluvní pokutu není omezeno ani jinak dotčeno právo kupujícího na náhradu škody vzniklé v příčinné souvislosti s porušením smluvní povinnosti prodávajícího v plné výši.

10.2. Pro případ prodlení s úhradou peněžitého závazku dle této Smlouvy si strany sjednávají úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i započatý, den prodlení.

10.3. V případě porušení povinnosti – nedodržení lhůty pro odstranění vady nebo vyřízení reklamace dle odst. 6. 3. této Smlouvy, resp. odst. 7.1 této Smlouvy se prodávající zavazuje zaplatit kupujícímu smluvní pokutu ve výši 2.000,- Kč za každý, byť i započatý den prodlení s odstraněním vady nebo vyřízením reklamace v každém jednotlivém případě. Tuto smluvní pokutu prodávající není povinen kupujícímu uhradit v případě, že místo platby této pokuty poskytne kupujícímu zdarma k plnému užívání náhradní plnění zcela srovnatelné s tím, na němž se vyskytla vada (závada), přičemž poskytnutím náhradního plnění kupující neztrácí právo na uhrazení této smluvní pokuty za počet dní, kdy kupující nemohl tohoto náhradního plnění plně užívat z důvodu na straně prodávajícího.

10.4. V případě porušení povinnosti – nepotvrzení přijetí oznámení reklamace či vady předmětu koupě dle odst. 6.2. této Smlouvy, resp. odst. 7.2. této Smlouvy se prodávající zavazuje zaplatit kupujícímu jednorázovou smluvní pokutu ve výši 1.000,- Kč za každý takový případ prodlení v každém jednotlivém případě nedodržení lhůty.

10.5. V případě porušení povinností stanovených ve čl. 8 této Smlouvy se prodávající zavazuje zaplatit kupujícímu smluvní pokutu ve výši 5.000,- Kč za každý, takový případ porušení smluvní povinnosti. Uplatněním práva na smluvní pokutu není omezeno ani jinak dotčeno právo kupujícího na náhradu škody vzniklé v příčinné souvislosti s porušením smluvní povinnosti prodávajícího v plné výši.

10.6. Pro jeden případ porušení povinností stanovených Smlouvou nelze kumulativně uplatnit více smluvních pokut.

10.7. Smluvní strany shodně prohlašují, že s ohledem na charakter povinností, jejichž splnění je zajištěno smluvními pokutami, jakož i s ohledem na charakter plnění zajišťovaného Prodávajícím dle Smlouvy, považují smluvní pokuty uvedené v tomto článku Smlouvy za přiměřené.

10.8. Vznikem povinnosti prodávajícího zaplatit kupujícímu smluvní pokutu ani zaplacením smluvní pokuty není dotčeno ani nijak omezeno právo kupujícího na náhradu škody vzniklé porušením povinnosti, jejíž splnění je zajištěno smluvní pokutou, v plném rozsahu.

10.9. Vznikem povinnosti prodávajícího zaplatit kupujícímu smluvní pokutu ani zaplacením smluvní pokuty nezaniká povinnost prodávajícího splnit povinnost, jejíž splnění bylo smluvní pokutou zajištěno; prodávající je i nadále povinen ke splnění takovéto povinnosti.

10.10. Vznikem povinnosti prodávajícího zaplatit kupujícímu smluvní pokutu ani zaplacením smluvní pokuty nezaniká právo kupujícího odstoupit od Smlouvy. Odstoupením od Smlouvy nezaniká nárok kupujícího na smluvní pokutu, k jejímuž zaplacení prodávajícímu již vznikla povinnost.

10.11. Smluvní pokuta je splatná do 21 dní od doručení písemného oznámení o jejím uplatnění prodávajícímu. Kupující je oprávněn svou pohledávku za prodávajícím z titulu povinnosti prodávajícího zaplatit smluvní pokutu započíst oproti pohledávce prodávajícího za kupujícím z titulu povinnosti kupujícího zaplatit kupní cenu.

11. Poskytnutí licence

11.1. Všechny komponenty předmětu koupě jsou dodávány včetně software. Pro případ, že hardware je dodáván včetně software, který je dílem, na které se vztahuje ochrana dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „Autorský zákon"), Prodávající tímto poskytuje kupujícímu oprávnění (licenci) užít tento software včetně jeho upgrade a update všemi způsoby užití, za účelem užívání dodaného hardware, resp. software.

11.2. Licence dle odst. 11.2. se sjednává jako časově neomezená v trvání po celou dobu autorské ochrany softwaru a pro území České republiky. Objednatel není povinen licenci využít.

11.3. Prodávající prohlašuje, že odměna za poskytnutí licence kupujícímu je již zahrnuta v kupní ceně za poskytnuté plnění dle této Smlouvy. Prodávající není oprávněn za poskytnutí licence požadovat úhradu žádných dalších či jiných plateb.

12. Vzájemná komunikace smluvních stran

12.1. Osoba oprávněná jednat za kupujícího v technických záležitostech týkajících se Smlouvy:

Bc. Miloslav Svoboda, vedoucí oddělení správy a rozvoje infrastruktury ICT

[redacted]

12.2. Osoba oprávněná jednat za prodávajícího v technických záležitostech týkajících se Smlouvy:

Ing. Tomáš ZLOCH, technický ředitel

[redacted]

12.3. Každá ze smluvních stran je oprávněna své kontaktní osoby jednostranně změnit, a to prostřednictvím písemného oznámení doručeného druhé smluvní straně. Změna je účinná okamžikem doručení oznámení druhé smluvní straně.

13. Ustanovení o vzniku a zániku Smlouvy

13.1. Smlouva nabývá platnosti dnem jejího uzavření. Dnem uzavření Smlouvy je den označený datem níže u podpisů smluvních stran. Pokud se data u podpisů smluvních stran liší, je dnem uzavření Smlouvy den označený pozdějším datem.

13.2. Smlouva nabude účinnosti dnem jejího uveřejnění v registru smluv dle § 6 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

13.3. Smlouva může být zrušena dohodou smluvních stran v písemné formě, přičemž účinky zrušení Smlouvy nastanou k okamžiku stanovenému v takovéto dohodě. Nebude-li takovýto okamžik dohodou stanoven, pak tyto účinky nastanou ke dni uzavření takovéto dohody. Takovou dohodou bude upraveno rovněž vypořádání případně již vzniklých závazků smluvních stran.

13.4. Kterákoliv ze smluvních stran je oprávněna od Smlouvy odstoupit v případech a za podmínek stanovených v § 2001 a násl. občanského zákoníku.

13.5. Kromě případů podle předchozího odstavce je prodávající oprávněn od Smlouvy bez dalšího odstoupit v případě, že kupující bude v prodlení s platbou kupní ceny delším než 14 dnů. Kromě případů podle předchozího odstavce je Kupující oprávněn od Smlouvy bez dalšího odstoupit v případě, že:

a) bude zjištěno nedodržení vlastností či parametrů prodávajícím dodaného předmětu koupě od těch, které jsou uvedeny v příloze č. 1 této Smlouvy,
b) prodávající bude v prodlení s dodáním předmět koupě delším než 14 dnů.

13.6. Odstoupení od Smlouvy musí být písemné a musí být doručeno druhé smluvní straně. Účinky odstoupení nastávají okamžikem doručení odstoupení druhé smluvní straně. Odstoupení od Smlouvy se nedotýká nároku na náhradu škody vzniklé porušením Smlouvy ani nároku na zaplacení smluvních pokut či úroku z prodlení.

13.7. V případě odstoupení od Smlouvy je smluvní strana, která již obdržela plnění od druhé smluvní strany, avšak sama plnění, ke kterému se Smlouvou zavázala, druhé smluvní straně ještě neposkytla, povinna toto plnění druhé smluvní straně vrátit bez zbytečného odkladu. Vrací-li plnění smluvní strana, která oprávněně odstoupila od Smlouvy, má tato smluvní strana nárok na náhradu nákladů s tím spojených. V ostatních případech jsou smluvní strany povinny vypořádat své vzájemné závazky vzniklé v souvislosti se Smlouvou do 30 dnů od účinnosti odstoupení.

13.8. Odstoupení od Smlouvy se nedotýká práva na zaplacení smluvní pokuty, dospělého úroku z prodlení, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany i po ukončení platnosti Smlouvy.

14. Prevence a detekce trestněprávních či neetických jednání, případná reakce na taková jednání

14.1. Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o této smlouvě vždy jednaly a postupovaly čestně a transparentně a současně se zavazují, že takto budou jednat i při plnění této smlouvy a veškerých činnostech s ní souvisejících.

14.2. Smluvní strany se dále zavazují vždy jednat tak a přijmout taková opatření, aby nedošlo ke vzniku důvodného podezření na spáchání trestného činu či k samotnému jeho spáchání (včetně formy účastenství), tj. jednat tak aby kterékoli ze smluvních stran nemohla být přičtena odpovědnost podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, nebo nevznikla trestní odpovědnost fyzických osob (včetně zaměstnanců) podle zákona č. 40/2009 Sb., trestního zákoníku, případně aby nebylo zahájeno trestní stíhání proti jakékoliv ze smluvních stran včetně jejích zaměstnanců podle platných právních předpisů.

14.3. Prodávající prohlašuje, že se seznámil se zásadami, hodnotami a cíli Criminal compliance programu Lesů České republiky, s.p. (viz www.lesycr.cz) (dále jen „CCP LČR"), zejména s

Kodexem CCP LČR, Protikorupčním programem LČR a Etickým kodexem zaměstnanců LČR včetně všech jejich příloh. Prodávající se při plnění této smlouvy zavazuje zásady a hodnoty CCP LČR dodržovat, a to po celou dobu jejího trvání, pokud to jejich povaha umožňuje.

14.4. Smluvní strany se dále zavazují navzájem si neprodleně oznámit důvodné podezření ohledně možného naplnění skutkové podstaty jakéhokoli z trestných činů, zejména trestného činu korupční povahy, a to bez ohledu a nad rámec případné zákonné oznamovací povinnosti; obdobné platí ve vztahu k jednání, které je v rozporu se zásadami vyjádřenými v tomto článku.

15. Závěrečná ustanovení

15.1. Smlouva se řídí právem České republiky. Práva a povinnosti Smlouvou výslovně neupravené se řídí občanským zákoníkem.

15.2. Veškeré spory vzniklé ze Smlouvy nebo v souvislosti s ní, které se nepodaří přednostně vyřešit smírně, budou rozhodovány obecnými soudy v souladu se zákonem č. 99/1963 Sb., občanským soudním řádem, ve znění pozdějších předpisů.

15.3. Žádná ze smluvních stran není oprávněna bez předchozího písemného souhlasu druhé smluvní strany převést na třetí osobu jakákoli práva nebo povinnosti vyplývající z této Smlouvy nebo postoupit na třetí osobu jakékoli pohledávky nebo dluhy vzniklé na základě této Smlouvy včetně práv, povinností, pohledávek nebo dluhů vzniklých na základě porušení této Smlouvy. Toto omezení nakládání s právy, povinnostmi, pohledávkami a dluhy trvá i po ukončení trvání této Smlouvy. Jakékoli právní jednání učiněné kteroukoli ze smluvních stran v rozporu s tímto omezením bude považováno za příčící se dobrým mravům.

15.4. Smlouva může být měněna pouze dohodou smluvních stran v písemné formě. Navrhne-li některá smluvní strana změnu Smlouvy, je druhá smluvní strana povinna se k takovému návrhu vyjádřit nejpozději do patnácti dnů ode dne doručení návrhu. Smluvní strany berou na vědomí, že případné změny Smlouvy musí být v souladu s právní úpravou zadávání veřejných zakázek

15.5. Prodávající bere na vědomí, že kupující bude postupovat v souladu se svými povinnostmi stanovenými v § 219 ZZVZ, tedy uveřejní na svém profilu zadavatele údaje a dokumenty, k jejichž uveřejnění je dle zmíněného ustanovení povinen. Prodávající souhlasí s uveřejněním Smlouvy, výše skutečně uhrazené ceny na základě Smlouvy.

15.6. Není-li ve Smlouvě pro konkrétní písemnost sjednáno něco jiného, pak platí, že právní účinky doručení jakékoli písemnosti doručované v souvislosti se Smlouvou či na jejím základě nastávají pouze tehdy, je-li tato písemnost odesílatelem či odesílatelem pověřeným provozovatelem poštovních služeb osobně předána jejímu adresátovi nebo je-li tato písemnost doručena jejímu adresátovi formou doporučeného psaní odeslaného prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence ve smyslu zákona č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů. Při doručování prostřednictvím osobního předání nastávají účinky doručení okamžikem písemného potvrzení adresáta o přijetí doručované písemnosti. Při doručování prostřednictvím doporučeného psaní nastávají účinky doručení okamžikem přijetí doručované písemnosti adresátem od poštovního doručovatele dle platných poštovních podmínek uveřejněných na základě zákona č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů. Doporučené psaní adresované smluvní straně je třeba adresovat vždy na adresu smluvní strany uvedenou ve Smlouvě. Tato doručovací adresa smluvní strany

může být změněna pouze písemným oznámením doručeným druhé smluvní straně. Pro doručování jiných poštovních zásilek než písemností platí toto ustanovení obdobně.

15.7. Smlouva se vyhotovuje ve čtyřech stejnopisech, přičemž každá ze smluvních stran obdrží po dvou z nich.

15.8. Smluvní strany prohlašují, že Smlouvu uzavírají svobodně a vážně, že považují obsah Smlouvy za určitý a srozumitelný a že jsou jim známy všechny skutečnosti, jež jsou pro uzavření Smlouvy rozhodující.

15.9. Nedílnou součástí Smlouvy jsou tyto její přílohy:

Příloha Smlouvy č. 1 – Technická specifikace
Příloha Smlouvy č. 2 – Ceník
Příloha Smlouvy č. 3 – Seznam členů realizačního týmu
Příloha Smlouvy č. 4 – Harmonogram

V Hradci Králové dne 12.10.2017

[redacted]

v zast.
správní ředitel
Ing. Igor Kalix, MBA

Lesy České republiky, s.p.
Ing. Daniel Szórád, Ph.D.
generální ředitel

Lesy České republiky, s.p. [26]
Přemyslova 1106/19, Nový Hradec Králové
500 08 Hradec Králové
IČ: 42196451, DIČ: CZ42196451

V Praze dne 10 -10- 2017

[redacted]

Huatech a.s.
Ing. Martin VÍTEK
jediný člen představenstva

HUATECH
Vyskočilova 741/3, 140 00 Praha 4
IČO: 03665496, DIČ: CZ03665496
info@huatech.cz
www.huatech.cz

LESY

Příloha č. 1 kupní smlouvy – Technická specifikace

1 TECHNICKÉ PARAMETRY ŘEŠENÍ

Řešení bude složeno ze dvou vzájemně propojených a integrovaných řešení:

- Systém pro uchování a agregaci logů zařízení perimetru s podporu automatizace reportů a centrální správy
- Systém pro monitoring a vyhodnocování toků v síti;
- Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik.

1.1 Systém pro agregaci logů bezpečnostního řešení perimetru s podporu automatizace reportů a centrální správy zařízení perimetru

Logovací a reportovací systém perimetru musí umožňovat bezztrátový sběr záznamů a incidentů zachycených bezpečnostními zařízeními perimetru. Zařízení musí umožňovat centralizovaný sběr ze všech zařízení perimetru a podporovat asynchronní režim minimalizující dopad na výkon monitorovaných zařízení a bezztrátový příjem událostí v případě vlastní zvýšené zátěže, např. při generování reportů.

Logovací a reportovací systém perimetru musí podporovat integraci s FW řešením včetně obousměrné komunikace logovacího systému s perimetrem (tj. logy uložené na logserveru musí být možné prohlížet přímo z MGMT rozhraní firewallu)

Uložení a uchování veškerých událostí a vygenerovaných reportů musí být zajištěno bezpečným lokálním úložištěm s podporou RAID technologie s dostatečnou kapacitou pro uložení veškerých záznamů po dobu několika měsíců a možností exportu na externí úložiště, nebo jako virtualní appliance s podporou instalace na RAID úložiště s dostatečnou kapacitou pro uložení veškerých záznamů po dobu několika měsíců a možností exportu na externí úložiště.

Možnost kumulativního rozšíření kapacity logovacího systému dle potřeby, bez závislosti na původní licenční politice.

Nad shromážděnými záznamy musí umožňovat prostřednictvím grafického webového prostředí parametrické vyhledávání, tvorbu agregovaných reportů, tvorbu uživatelských reportů a plánování automatizace reportovacích úloh včetně automatického odesílání vytvářených reportů a analýz ve formátech umožňujících jejich zobrazení a uložení mimo vlastní prostředí systému – minimálně PDF sestavy odesílané formou emailových zpráv.

Řízení přístupu k zařízení musí podporovat správu minimálně na úrovni rolí uživatel a správce. Reportovací nástroje musí umožňovat analýzy poskytující úplný přehled bezpečnostních hrozeb detekovaných bezpečnostním řešením perimetru a veškerých systémových událostí v těchto zařízeních včetně změn v administrátorských oprávněních v uživatelsky definovaných intervalech.

Systém centrální správy perimetru musí umožňovat centralizované nasazování bezpečnostních politik, konfigurací a aktualizací. Plnou podporu a integraci stávajících zařízení perimetru, virtuálních domén, user identity management systému a logovacímu a reportovacímu systému.

Možnost kumulativního rozšíření systému centrální správy perimetru o další zařízení dle potřeby, bez závislosti na původní licenční politice.

Systém centrální správy perimetru musí umožňovat správu zařízení prostřednictvím grafického webového prostředí, možnost auditu konfiguračních změn, řízení přístupu administrátorů na různých

úrovních oprávnění a real-time monitoring a reporting nad spravovanými zařízeními a událostmi perimetru.

Zadavatel požaduje minimálně následující parametry pro Logovací a reportovací systém perimetru

Název požadavku	Popis požadavku	Míra splnění
Hlavní funkcionalita	Sběr logů a systémových událostí, z centrálních UTM. Analýza a vizualizace událostí perimetru. Využití kapacity a výkonnostních charakteristik perimetru. Uchování záznamů o provozu perimetru, bezpečnostních incidentů v souladu se zákonem 181/2014 a související legislativou.	ANO
Denní log kapacita	Minimální denní přírůstek logů v 26GB/Day	ANO
Kapacita úložiště	Minimální kapacita úložiště 10TB	ANO
Podpora RAID	Podpora RAID Level 0/1/5/10	ANO
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.	ANO
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.	ANO
VM Appliance	V případě virtuální appliance podpora VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2	ANO
Podpora VDOM	Podpora VDOM virtuálních domén	ANO
Komunikace s perimetrem	Plnou integraci s FW řešením, včetně obousměrné komunikace (tj. logy uložené na logserveru musí být možné prohlížet přímo z MGMT rozhraní firewallu)	ANO
Rozšíření kapacity úložiště	Možnost kumulativního rozšíření kapacity úložiště, ke stávajícím 10TB.	ANO
Výrobcem předpřipravené reporty	Široká nabídka předpřipravených reportů (nejčastěji využívaných reportů- bezpečnostní incident, využití konektivity, navštěvované kategorie stráne, atd.)	ANO
Vlastní reporty	Možnost tvorby vlastních detailních reportů	ANO
Export reportů	Možnost exportu reportů (HTML, PDF, CSV, XML)	ANO
Vyhodnocování událostí a systém upozornění	Podpora vyhodnocování událostí a upozornění na ně (email, snmp trap) Možnost vlastní definice monitorovaných událostí	ANO
Podpora multi-tenantního prostředí	Oddělené rozhraní na log/reporting server pro různé virtuální FW	ANO
Podpora výrobce	Podpora výrobce v režimu 24x7 po dobu 2 let	ANO

Zadavatel požaduje minimálně následující parametry pro systém centrální správy perimetru

Název požadavku	Popis požadavku	Míra splnění
Hlavní funkcionalita	Systém centrální správy perimetru musí umožňovat centralizované nasazování bezpečnostních politik, konfigurací a aktualizací. Plnou podporu a integraci stávajících zařízení perimetru, virtuálních domén, user identity management systému a logovacímu a reportovacím systému.	ANO
Počet zařízení ve správě	Správa minimálně 10 Fortinet zařízení/virtuálních domén	ANO
Denní log kapacita	Minimální denní přírůstek logů v 1GB/Day	ANO
Kapacita úložiště	Minimální kapacita úložiště 100 GB	ANO
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.	ANO
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.	ANO
VM Appliance	V případě virtuální appliance podpora VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2	ANO
Podpora VDOM	Podpora VDOM virtuálních domén	ANO
Rozšíření kapacity spravovaných zařízení	Možnost kumulativního rozšíření systému centrální správy perimetru o další zařízení ke stávajícím 10.	ANO
Podpora výrobce	Podpora výrobce v režimu 24x7 po dobu 2 let	ANO

1.2 Systém pro monitoring a vyhodnocování toků v síti

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Uložení a zpracování statistik musí být redundantní na k tomu určených specializovaných zařízeních – kolektorech. Ty musí být vybaveny SW či HW RAIDem. Kolektory musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat musí probíhat kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Samozřejmostí bude plná customizace způsobu prezentace dat a reportů na základě cílového prostředí.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow). Tato technologie představuje nejmodernějším prostředek pro monitorování sítě při zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě.

Systém pro monitoring a vyhodnocování toků v sítise bude skládat ze dvou na sobě nezávislých částí:

- Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat;
- Fyzické sondy pro sběr dat z prvků nepodporující export flow záznamů

1.2.1 Kolektor s detekcí anomálií

Kolektor bude splňovat minimálně následující parametry:

Název požadavku	Popis požadavku	Míra splnění
Ukládání flow statistik	Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce.	Ano
Granularita vizualizace	Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5-minutových nebo 30-sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků.	Ano
Podpora standardů datových toků	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite.	Ano
Hlavní funkcionalita	Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.	Ano
Instalace	Snadná instalace do stávající síťové infrastruktury – racková montáž, maximálně 2U	Ano, 2U
Management rozhraní	Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat.	Ano, 2x Base-T
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.	Ano, HTTPS a SSL
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.	Ano
LDAP autentizace	Podpora autentizace vůči LDAP (Active Directory).	Ano
TACACS+ autentizace	Podpora autentizace vůči TACACS+.	Ano
Podpora HOT SWAP a RAID	Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce.	Ano,RAID6
Dohled	Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.	Ano
Časová synchronizace	Časová synchronizace zařízení proti centrálnímu zdroji času na síti.	Ano
Podpora příkazové řádky	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.	Ano
Sériová linka pro konfiguraci zařízení	Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232).	Ano Ano
DNS cache	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.	Ano
Podpora Cisco AVC	Podpora standardu Cisco AVC vč. položek HTTP hostname a URL.	Ano
Podpora dalších flow standardů	Podpora pro Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2.	Ano
Podpora položek proměnlivé délky	Podpora IPFIX položek proměnlivé délky.	Ano
Monitoring výkonu sítě	Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.	Ano

Název požadavku	Popis požadavku	Míra splnění
Monitoring informací z aplikační vrstvy	Podpora pro protokoly HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP	Ano
Monitorování rozšířených L3/L4 informací	Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů.	Ano
Přeposílání flow vč. možnosti samplingu	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků.	Ano
Spolehlivý a šifrovaný přenos IPFIX dat	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS).	Ano
Automatická identifikace zdroje flow statistik	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.	Ano
Zálohování a obnova flow statistik	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.	Ano
Podpora pro uživatelské identity	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele).	Ano
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel).	Ano
Vizualizace statistických dat	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem.	Ano
Analýza dat a ad hoc výstupy	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.	Ano PDF a CSV
Reporting	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.	Ano
Řízení uživatelského přístupu	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).	Ano
Top N statistiky	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.	Ano
Filtrování a přizpůsobení výstupů	Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat	Ano

Název požadavku	Popis požadavku	Míra splnění
	do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).	
Uživatelsky definovatelné alerty	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.	Ano
Uživatelsky definované pohledy na datový provoz	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.).	Ano
Drill-down	Možnost dohledat každý jednotlivý datový tok (flow záznam).	Ano
Monitoring aktivních zařízení na síti	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení.	Ano
Automatická podpora geolokace	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).	Ano
Otevřené rozhraní	Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).	Ano
Aplikace pro mobilní zařízení	Aplikace pro mobilní zařízení platformy Android a iOS, pro zobrazování základních informací v podobě grafů a statistik per jednotlivý uživatel.	Ano
Monitorování dostupnosti zdroje flow dat	Monitorování dostupnosti zdroje flow dat pomocí SNMP.	Ano
Minimální velikost interního datového úložiště	12 TB čisté kapacity na HW RAID6	Ano, 12TB
Minimální velikost RAM paměti kolektoru	64GB RAM	Ano, 64GB RAM
Minimální počet toků/s který je kolektor schopen zpracovat	200.000 toků/s	Ano, 250 000 toků

Systém pro automatické vyhodnocování a monitoring IP toků musí umožnit automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách tzv. behaviorální analýzy a umožňovat tak odhalování hrozeb a incidentů, které překonají zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplní stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události bude možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů výrazně přispěje ke zjednodušení správy datové sítě, zvýšení její bezpečnosti a umožní proaktivní identifikaci příčin problémů.

Systém pro automatickou detekci musí být plně integrovatelný do prostředí kolektoru, tak aby mohl uživatel pracovat pouze s jedním GUI.

Název požadavku	Popis požadavku	Míra splnění
Podpora flow standardů	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream.	Ano
Deduplikace	Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.	Ano
Korelace před a za proxy	Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli.	Ano
Vzorkování na úrovni toků	Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním.	Ano
Identita uživatelů	Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události.	Ano
Persistence doménových jmen	Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události.	Ano
Detekční pravidla a algoritmy	Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií.	Ano
Detekce síťových útoků	Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.	Ano
Detekce anomálií v síťovém provozu	Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.	Ano
Detekce nežádoucích aplikací	Detekce P2P sítí, a anonymizačních služeb (např. TOR)	Ano
Detekce událostí na základě „Threat intelligence" dat	Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci.	Ano
Detekce provozních problémů	Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti.	Ano
Detekce síťových anomálií	Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace.	Ano
Konfigurační průvodce	Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen.	Ano
Konfigurace detekčních schopností	Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ).	Ano
Detekce NATů	Detekce NATů v síti s využitím rozšířených informací z L3/L4.	Ano
Správa filtrů	Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu CSV nebo z tohoto formátu importovat.	Ano

Název požadavku	Popis požadavku	Míra splnění
Správa falešných poplachů	Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní.	Ano
Definice závažnosti událostí	Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit.	Ano
Agregace událostí	Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.).	Ano
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele.	Ano
CEF export	Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management.	Ano
SNMP Trap	Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap.	Ano
E-mailové notifikace	Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu.	Ano
Záchyt provozu v plném rozsahu	Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu.	Ano
Spuštění skriptu	Na výskytu události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů.	Ano
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí.	Ano
Integrace informací z jiných služeb	Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP.	Ano
Kategorie a komentáře	Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře.	Ano
Vyhledávání událostí	Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.).	Ano
Interaktivní vizualizace událostí	Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána.	Ano
Reporting	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem.	Ano
CSV export	Události je možné exportovat do formátu CSV pro další zpracování.	Ano
Otevřené rozhraní	Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné	Ano

Název požadavku	Popis požadavku	Míra splnění
	systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).	
Sledování změn konfigurace	Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management.	Ano
Formát systémů	Systém musí běžet na HW zařízení kolektoru, musí být dostupný přes jednotné WEB GUI kolektoru	Ano
Výkon systému	Systém musí být schopen vyhodnotit minimálně 3 tisíce toků za vteřinu	Ano, 3 000
Počet zdrojů	Systém musí umět pracovat minimálně se třemi nezávislými zdroji dat (Flow instance)	Ano, 3
GUI systému	GUI musí být k dispozici v českém a anglickém jazyce	Ano

1.2.2 Fyzické sondy pro sběr dat

Fyzické sondy budou splňovat minimálně následující parametry:

Zdroje NetFlow/IPFIX dat (sondy) jsou výkonná autonomní zařízení, která monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data obsahují informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvy OSI modelu. Sondy rovněž umožňují analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu poskytují sondy rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti. Díky tomu přináší sonda komplexní přehled a detailní informace o dění v síti a usnadňuje tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Sondy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňují sledovanou síť. K síti musí být připojeny pasivně prostřednictvím SPAN/mirroring portu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné.

Obecné požadavky na sondy:

Název požadavku	Popis požadavku	Míra splnění
Pasivní zapojení	Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty).	Ano
Instalace	Snadná instalace do stávající síťové infrastruktury – hardwarové zařízení, maximální velikost 1U	Ano, 1U
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.	Ano
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí.	Ano
Dohled	Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.	Ano
Časová synchronizace	Časová synchronizace zařízení proti centrálnímu zdroji času na síti.	Ano
Podpora příkazové řádky	Jednoduchá instalace a nastavení zařízení prostřednictvím GUI. Základní správa prostřednictvím příkazové řádky a GUI.	Ano
DNS cache	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.	Ano
LDAP autentizace	Podpora autentizace vůči LDAP (Active Directory).	Ano

Název požadavku	Popis požadavku	Míra splnění
Podpora protokolů pro výměnu dat	Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX.	Ano
Zpracování datového provozu	Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.	Ano
Analýza tunelovaného provozu	Monitorování provozu v tunelu GRE.	Ano
Uživatelsky definované šablony	Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX.	Ano
Monitorování MAC adres	Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu.	Ano
Detekce aplikací	Detekce aplikací dle standardu NBAR2.	Ano
Analýza zpoždění na síti	Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Monitorování a analýza HTTP provozu	Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Profilování zařízení v síti	Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Monitorování VoIP	Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Monitorování DNS provozu	Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Monitorování Samba/CIFS provozu	Monitorování a analýza Samba/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Monitorování DHCP provozu	Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	Ano
Nastavení času pro expiraci toků	Podpora pro nastavení časů u aktivní a neaktivní expirace toků.	Ano
Vzorkování	Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků.	Ano
Simultánní export NetFlow statistik	Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX).	Ano
Export na základě filtrování dat na sondě	Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky).	Ano

Název požadavku	Popis požadavku	Míra splnění
Vyplňování identifikace AS	Podpora vyplňování AS na základě vestavěného či dodaného seznamu.	Ano
Vyplňování čísla interface	Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port.	Ano
Záchyt provozu v plném rozsahu	Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace.	Ano
Monitorování rozšířených L3/L4 informací	Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.	Ano
TACACS+ autentizace	Podpora autentizace vůči TACACS+.	Ano
GUI systému	GUI musí být k dispozici v českém a anglickém jazyce	Ano

1G Sonda

Název požadavku	Popis požadavku	Míra splnění
Kapacita paměti současných toků	Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port.	Ano, 500 000
Monitorovací porty sond	Sonda obsahuje minimálně 4x 1GbE monitorovacích portů – rozhraní RJ45	Ano, 4x 1G Base-T
Výkon sondy na 1GbE monitorovacími porty	Sondy jsou schopné zpracovávat více než 1,4Mp/s (pakety za sekundu) na každém portu	Ano, 1,48Mp/s

10G Sonda

Název požadavku	Popis požadavku	Míra splnění
Kapacita paměti současných toků	Minimální kapacita paměti současných toků na sondě 4 miliony toků per monitorovací port.	Ano, 4 000 000
Monitorovací porty sond	Sonda obsahuje minimálně 2x 2 10GbE monitorovacích portů - rozhraní SFP+	Ano, 2x 10G Base-X SFP+
Výkon sondy na 1GbE monitorovacími porty	Sondy jsou schopné zpracovávat více než 1,4Mp/s (pakety za sekundu) na každém portu	Ano 1,5Mp/s

1.3 Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik

Nástroj pro zajištění centrální správy IP adresního prostoru musí obsahovat integrované nástroje základních síťových služeb DNS a DHCP, L2 monitoring sítě a řízení přístupu do sítě (NAC - založený na standardu radius) – s jednotnou uživatelskou správou přes GUI.

Systém na vzdálených lokalitách (lokalitách krajských ředitelství) musí obsahovat systém pro generování Flow dat se stejným výstupem jako hardwarové sondy poptávané v části 1.1.

Požadavky na celý systém jsou rozděleny do několika částí, ale ve výsledku tvoří jeden funkční celek s unifikovaným a jednotným GUI.

1.3.1 Obecné požadavky na systém

Definice požadavku	Míra splnění
Řídící servery systému musí podporovat možnost provozu ve virtuálním prostředí (VMware)	Ano
Výkonné servery ve formě fyzických appliancí musí využívat zabezpečený operační systém, být schopné poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti)	Ano, celkem 6 centrálních serverů a 12 pobočkových
Systém appliancí musí podporovat možnost nasazení v on-line clusteru a podporovat vícenásobnou redundanci i přes různé lokality	Ano
Možnost rozšíření funkčního rozsahu appliancí o sběr NetFlow/IPFIX dat o provozu ve vzdálených lokalitách a jejich odesílání do centrálního kolektoru monitorovacího systému	Ano, na všech 12 vzdálených lokalitách
Systém musí obsahovat samostatný systém pro centrální správu a nastavení appliancí	Ano. Web GUI
Systém musí být schopen integrace se systémy pokročilé síťové analýzy (NBA) nebo SIEM	Ano
Systém musí podporovat možnost napojení na SMS bránu pro odesílání autentizačních informací uživatelům	Ano, možnost rozšíření
GUI systému musí být k dispozici v českém a anglickém jazyce	Ano

1.3.2 Systém pro adresní plánování

Definice požadavku	Míra splnění
Je nástrojem pro návrh a definici IP adresního plánu s možností definice sítí, výběr konkrétní sítě a práce s ní	Ano
Systém musí podporovat v sítích možnost definice bloků adres, výběry dle bloků adres	Ano
Systém musí podporovat import MAC/IP adres z online monitoringu sítě, automatický výběr správné sítě pro importované adresy	Ano
Systém musí podporovat import/export záznamů do/z adresního plánování v XML nebo CSV formátu	Ano
Systém musí podporovat automatické generování pravidel pro DHCP servery z adresního plánování	Ano
Systém musí podporovat automatické vytváření DNS záznamů z adresního	Ano
Systém musí podporovat vytváření profilů dle sítí, po výběru profilu zobrazení a možnost práce pouze s IP adresami sítí daných profilem	Ano
Systém musí podporovat nástroj pro hromadné práce s definovanými skupinami zařízení a podporu krizového řízení	Ano

1.3.3 Systém pro monitoring sítě

Definice požadavku	Míra splnění
Systém musí podporovat monitoring na L2 vrstvě - MAC a IP adres v reálném čase, včetně toho, na kterém fyzickém portu switche se daná MAC adresa nachází, pokud	Ano

Definice požadavku	Míra splnění
switch tuto možnost poskytuje (na kterém portu kterého switche je připojené zařízení s danou MAC adresou), včetně podpory historie	
Systém musí podporovat dostupnost monitoringu i v lokalitách, kde je přístup přes třetí vrstvu (routované lokality), data musí být online k dispozici přes uživatelské rozhraní na centrální lokalitě	Ano
Systém musí podporovat online sledování a vyhodnocení monitoringu ve formě: povolená dvojice MAC-IP, zakázaná dvojice MAC-IP, nekorektní DHCP MAC-IP, neznámá MAC-IP	Ano
Systém musí podporovat vypsání „mrtvých" MAC nebo IP adres (adresy, které se v síti nevyskytly např. půl roku), s možností přes uživatelské rozhraní provést vymazání z DHCP, DNS a Radius záznamů a vrácení příslušných IP adres do adresního plánování	Ano
Systém musí podporovat export odmonitorovaných záznamů do XML nebo CSV	Ano, XML i CSV

1.3.4 Integrovaný DHCP server

Definice požadavku	Míra splnění
Musí se jednat o distribuovaný DHCP systém s možností existence více DHCP serverů na stejné síti (redundance)	Ano, vždy redundatně
Systém musí podporovat centrální řízení a zakládání pravidel	Ano
Systém musí podporovat redundanci řídícího serveru, nezávislé na lokalitě	Ano
Systém musí podporovat uživatelsky definované DHCP volby	Ano
Systém musí podporovat definice adresních skupin, k nim vázané DHCP volby	Ano
Systém musí podporovat vytvoření DHCP pravidla s vazbou více MAC na více IP adres	Ano
Systém musí podporovat možnost definice i statického záznamu (pro danou MAC není přidělovaná adresa DHCP serverem, pouze existuje záznam pro Radius server a monitoring, že daná MAC a IP adresa je na síti platná)	Ano
Systém musí podporovat možnost existence DHCP záznamů jedné MAC adresy ve více různých sítích - v každé síti obdrží daná MAC adresa přesně svou IP adresu z rozsahu dané sítě - cestující uživatelé	Ano
Systém musí podporovat automatické vytvoření/změna/smazání DHCP záznamu při operacích v adresním plánování	Ano
Systém musí podporovat automatickou propagaci MAC adres z DHCP záznamů v uživatelsky definovaném formátu do Radius serverů pro realizaci dalších bezpečnostních mechanizmů prostřednictvím aktivních prvků sítě (podpora heterogenních aktivních prvků pro 802.1x autentizaci)	Ano

1.3.5 Integrovaný DNS server

Definice požadavku	Míra splnění
Systém musí podporovat centrální řízení a zakládání pravidel	Ano
Systém musí podporovat automatické vytváření A a PTR záznamů z adresního plánování	Ano
Centrální řídící server musí mít redundanci nezávislou na lokalitě	Ano
Systém musí podporovat možnost rozdělení zón na vnitřní a vnější pro stejnou zónu, definice vazby na vnitřní nebo vnější zónu dle IP adres (sítí) DNS klientů (klienti ve vnější síti dostávají odpovědi pouze pro DNS záznamy z vnější zóny, klienti z vnitřní zóny dostávají DNS odpovědi pro vnitřní i vnější zónu)	Ano, včetně propojení s MS AD
Systém musí podporovat replikaci zvolených zónových souborů na podřízený DNS server	Ano
Systém musí podporovat automatického vytváření PTR reverzních záznamů při zakládání "A" záznamů	Ano
Systém musí podporovat porovnání DNS z Adresního plánování s DNS záznamy na DNS serveru, včetně automatizovaného nástroje pro řešení rozdílů	Ano

1.3.6 Bezpečnostní část/NAC

Definice požadavku	Míra splnění
Systém musí podporovat řízení přístupu do sítě s využitím 802.1x/MAC autentizace a následné Autorizace (dynamické přidělení VLAN)	Ano, podporují ve spolupráci s Huawei přepínači
Systém musí podporovat krizové řízení – schopnost hromadné deaktivace síťové komunikace pro všechny zařízení mimo vyjmenovanou kritickou infrastrukturu organizace	Ano
Systém musí podporovat uživatelské rozhraní s možností přidělování různých stupňů oprávnění. Audit musí být schopen zaznamenat minimálně kdo, kdy a jaké typy operací v systému prováděl	Ano
Systém musí podporovat sledování incidentů na síti s možností generování bezpečnostních reportů	Ano

1.3.7 Spolupráce s aktivními prvky Huawei nasazenými v prostředí LČR

Definice požadavku	Míra splnění
Systém musí podporovat automatické zálohování konfigurací aktivních prvků	Ano
Systém musí podporovat sledování výskytu MAC adres na portech s historií pro účely určení, kde se v daném čase vyskytuje nebo vyskytovala MAC adresa	Ano
Systém musí podporovat automatické repository - informace o verzi firmware, typu zařízení, S/N apod.	Ano
Systém musí podporovat sledování využití portů síťových prvků v čase - detekce nepoužívaných	Ano

1.3.8 BYOD část – plná spolupráce s Huawei WiFi řešením nasazeným v prostředí LČR

Definice požadavku	Míra splnění
podporovaná veškerá funkcionalita rovněž pro mobilní zařízení s přístupem přes WiFi	Ano
podpora samoobslužného rozhraní pro automatizovanou IP správu nových zařízení v síti	Ano
možnost vytváření recepčních zón pro zajištění přístupů návštěv (Guest zóna)	Ano

1.4 Školení

Prodávající provede pro kupujícím určené osoby:

- Uživatelské školení pro systém Monitoringu a vyhodnocování toků v síti (rozsah 1MD), počet účastníků až 20;
- Administrátorské školení pro systém Monitoring a vyhodnocování toků v síti (rozsah 3MD), počet účastníků až 4;
- Uživatelské školení pro systém Monitoring sítě, správu adresního prostoru a systém řízení přístupových politik (rozsah 1MD), počet účastníků až 20;
- Administrátorské školení pro systém Monitoring sítě, správu adresního prostoru a systém řízení přístupových politik (rozsah 2MD), počet účastníků až 4.

1.5 Definice rozsahu nasazení

Systém bude nasazen v následujícím rozsahu:

1.5.1 Systém pro monitoring a vyhodnocování toků v síti

Systém (kolektor a sondy) bude nasazen centrálně na úrovni generálního ředitelství vč. centrálního datového centra.

Na úrovni krajských řešení bude jakoukoliv dodávanou komponentou nabízeného řešení zajištěn systémem pro sběr NetFlow/IPFIX dat o provozu.

1.5.2 Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik

Systém podporující redundanci a distribuovanost služeb L2 monitoringu a DHCP/DNS/NAC pro následující lokality, které budou vybaveny hardwarovým řešením:

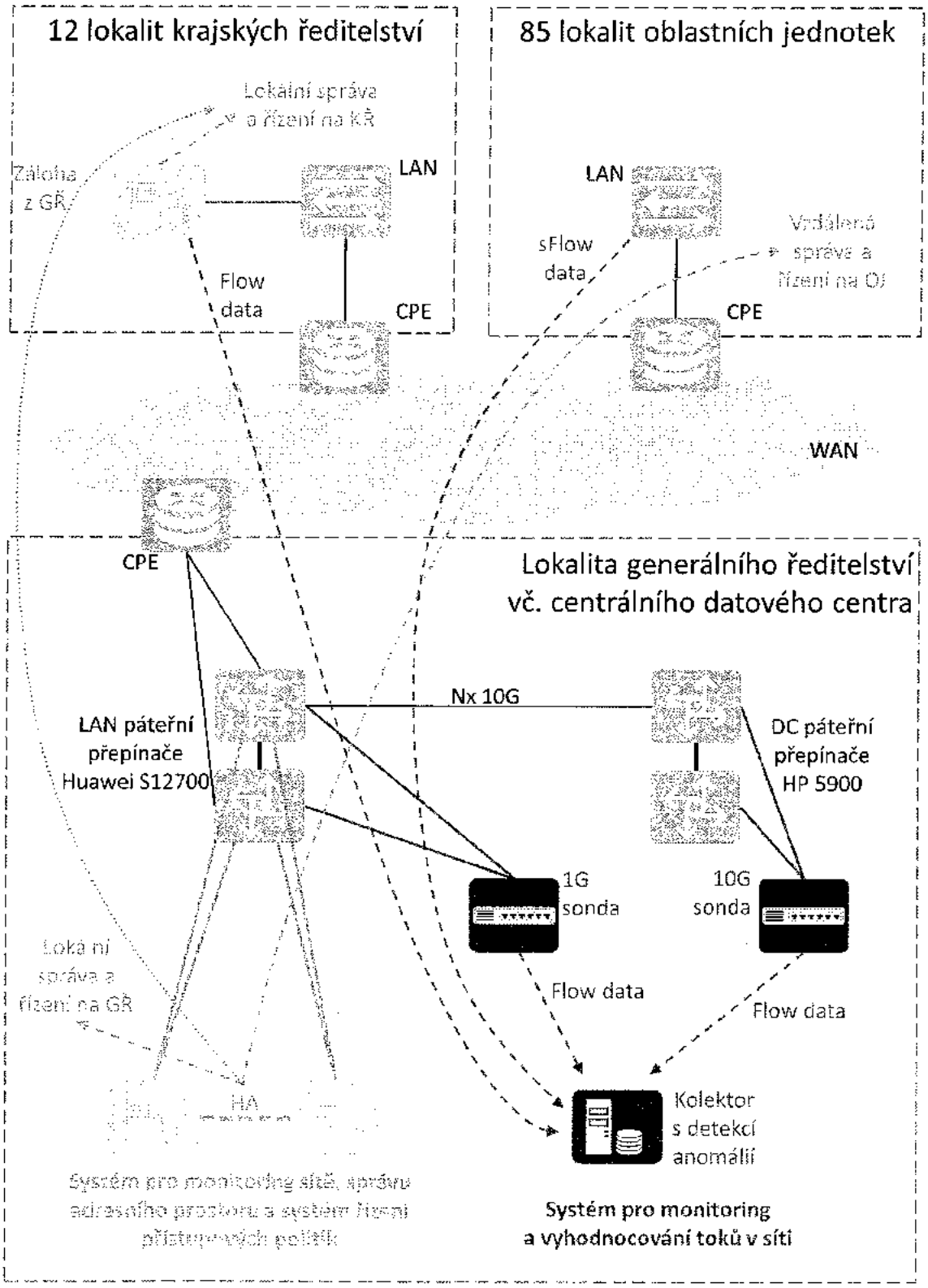
- Lokalita generálního ředitelství vč. centrálního datového centra;
- 12 dalších lokalit krajských ředitelství.

Dalších 85 lokalit oblastních jednotek, bude řešeno centralizovaným modelem nasazených služeb L2 monitoringu a DHCP/DNS/NAC z lokality GŘ.

Celkové množství spravovaných zařízení bude cca do 5.000 IP zařízení v síti.

1.5.3 Blokové schéma řešení

Nabízené řešení musí reflektovat požadavky na instalaci a implementaci v prostředí sítě kupujícího, které vyplývají z následujícího blokového schématu:


12 lokalit krajských ředitelství
Lokální správa a řízení na KŘ
Záloha z GŘ
LAN
Flow data
CPE
85 lokalit oblastních jednotek
LAN
sFlow data
Vzdálená správa a řízení na OJ
CPE
WAN
CPE
Lokalita generálního ředitelství vč. centrálního datového centra
Nx 10G
LAN páteřní přepínače Huawei S12700
DC páteřní přepínače HP 5900
1G sonda
10G sonda
Lokální správa a řízení na GŘ
Flow data
Flow data
HA
Kolektor s detekcí anomálií
Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik
Systém pro monitoring a vyhodnocování toků v síti

2 DETAILNÍ POPIS NABÍZENÉHO PLNĚNÍ

2.1 Systém pro agregaci logů bezpečnostního řešení perimetru s podporu automatizace reportů a centrální správy zařízení perimetru

FortiAnalyzer je nástroj pro analýzu sítě, logování síťového provozu a nástroj pro vytváření cílových reportů ze získaných logů. Administrátorům sítě přináší hluboký a ucelený přehled o síťovém provozu.

Popis zařízení – FortiAnalyzer FAZ-VM-GB25 je multiplatformní virtuální appliance s možností uchování až 10,5 TB logů a kapacitou 26GB/logů za den. Tento výkon/kapacita lze použít pro sběr dat Fortinet produktů, tak i ze zařízení třetích stran pomoci protokolu syslog.

FortiAnalyzer podporuje asynchroní režim sběru dat a minimalizuje dopad na výkon monitorovaných zařízení a bez-ztrátový příjem událostí v případě vlastní zvýšené zátěže. Je schopen obousměrné komunikace se zařízením FortiGate a administrátor tak získává celkový přehled o síťových incidentech/událostech z managemantu samotného firewalu.

FortiAnalyzer disponuje nástrojem Vulnerability management, který nabízí rozšířené skenování celé sítě a systémů. Využívá k tomu sady dynamických signatur, které detekují zařízení v síti a hledají jejich možná zranitelná místa.

Klíčové vlastnosti:

- Korelace síťových událostí (umožňuje IT administrátorům rychle identifikovat a efektivněji reagovat na bezpečnostní hrozby v rámci sítě)
- Jednodušší grafické reporty (poskytuje široké spektrum reportů událostech, aktivitách uživatelů a trendů vyskytujících se v síti)
- Škálovatelný výkon a kapacita
- Centralizovaný monitorovací a logovací nástroj pro více typů záznamů (FortiAnalyzer je schopný analyzovat informace přímo z datových přenosů, systémových událostí, výskytů virů, útoků, událostí webové filtrace, e-mailů a instant messagingu)
- Bezproblémová integrace s ostatními Fortinet produkty (mezi FortiAnalyzer produkty a ostatními Fortinet appliance existuje přímá integrace, která umožňuje maximalizovat výkon a spolupracovat s FortiAnalyzer přímo z FortiGate nebo FortiManager zařízení)

2.2 Systém pro monitoring a vyhodnocování toků v síti

Monitorování počítačových sítí na bázi datových toků (standardy NetFlow/IPFIX a další) je základem moderní správy IT prostředí. Nástroje využívající tuto technologii významně usnadňují diagnostiku, optimalizaci výkonu sítě, identifikaci a troubleshooting provozních problémů a další úkoly. Šetří čas i náklady a přináší řadu benefitů všem typům společností, od těch menších, až po velké firmy a organizace.

Využití monitorování datových toků v oblasti bezpečnosti, tzv. detekce anomálií a analýza chování sítě (Network Behavior Anomaly Detection, NBAD) navíc otevírá úplně nové možnosti pro zajištění ochrany cenných podnikových dat a systémů před pokročilými hrozbami, které obchází tradiční bezpečnostní prvky, jako jsou firewall, IDS/IPS systém nebo antivirus.

Nabízené řešení Flowmon přináší absolutní viditelnost síťového provozu a řadu funkcí pro optimalizaci výkonnosti sítí a aplikací a ochranu před moderními kybernetickými hrozbami. Využívá přitom

technologii monitorování datových toků (NetFlow/IPFIX) a pokročilou umělou inteligenci pro detekci anomálií a analýzu chování sítě.

Flowmon od začátku do konce pokrývá proces monitorování sítí. Zahrnuje nejvýkonnější síťové sondy pro export NetFlow/IPFIX statistik na světě, kolektory určené k uložení, vizualizaci a analýze statistik, a specializované moduly pro pokročilé analytické funkce. Díky tomu, že Flowmon využívá informace z vrstvy L7, dovoluje uživateli vyřešit až 95 % provozních problémů v síti jedním produktem!

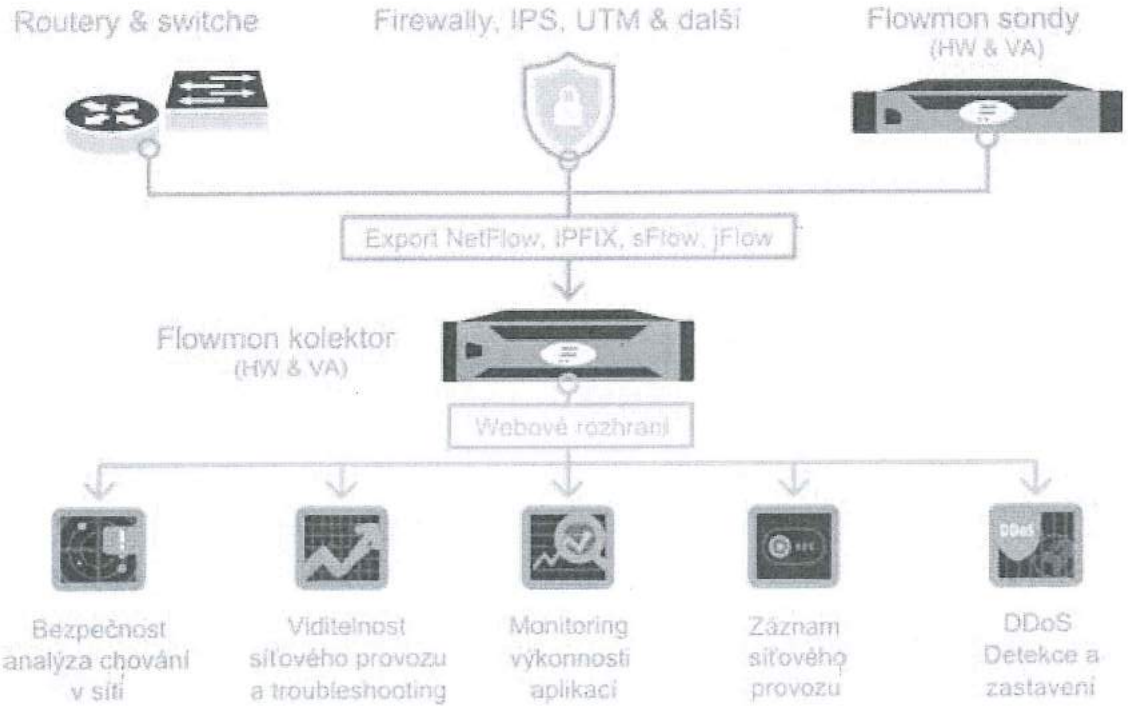
Nabízené řešení se skládá z následujících komponent:

- Flowmon kolektor - Flowmon Collector R6-12000 Pro
- Licence na Flowmon ADS - FPC-ADS-C verze Corporate
- Dvě HW sondy: Flowmon Probe 4000 a Flowmon Probe 20000 SFP+

Popis zařízení - Flowmon kolektor - Flowmon Collector R6-12000 Pro

Flowmon kolektor poskytuje správcům sítí a bezpečnostním expertům detailní viditelnost do síťového provozu. Toto výkonné zařízení umožňuje sběr, zobrazení, analýzu a dlouhodobé uložení statistik o komunikaci v síti (ve standardech NetFlow v5/v9, IPFIX, sFlow a dalších), které generují switche, routery, síťové sondy či jiné zdroje. Díky přehlednému uživatelskému rozhraní získávají administrátoři absolutní kontrolu nad sítí a mocný nástroj pro řešení provozních/bezpečnostních incidentů a zvýšení výkonnosti nejen sítě, ale také aplikací. Funkce Flowmon kolektoru dále rozšiřují specializované moduly pro pokročilou analýzu datových toků. Patří k nim Flowmon ADS pro detekci anomálií a analýzu chování v síti, Flowmon APM pro zlepšování kvality aplikací, Flowmon Traffic Recorder pro kompletní záznam datové komunikace a Flowmon DDoS Defender pro detekci a zastavení DDoS útoků.

Všechny modely kolektorů jsou vybaveny aplikací Flowmon monitorovací centrum (FMC), profesionálním nástrojem pro efektivní analýzu síťových statistik. Aplikace je optimalizovaná pro ukládání a zpracování velkého množství statistických dat. Zachycené statistiky jsou intuitivně zobrazovány v přehledných grafech a tabulkách s možností volby perspektivy a časových období. FMC navíc umožňuje nad zaznamenanými daty definovat pokročilé filtry, pomocí kterých lze rychle najít konkrétní komunikaci, incident nebo anomálii. Zachycená data ze sond a dalších zařízení ukládá FMC ve formátu definovaném aplikací NfDump, což zajišťuje kompatibilitu s celou řadou dalších aplikací pro NetFlow analýzu. Tím umožňuje zákazníkům tyto aplikace jednoduše kombinovat. Samozřejmostí je možnost definovat automatická upozornění na nežádoucí situace a anomálie (viry, p2p apod.).

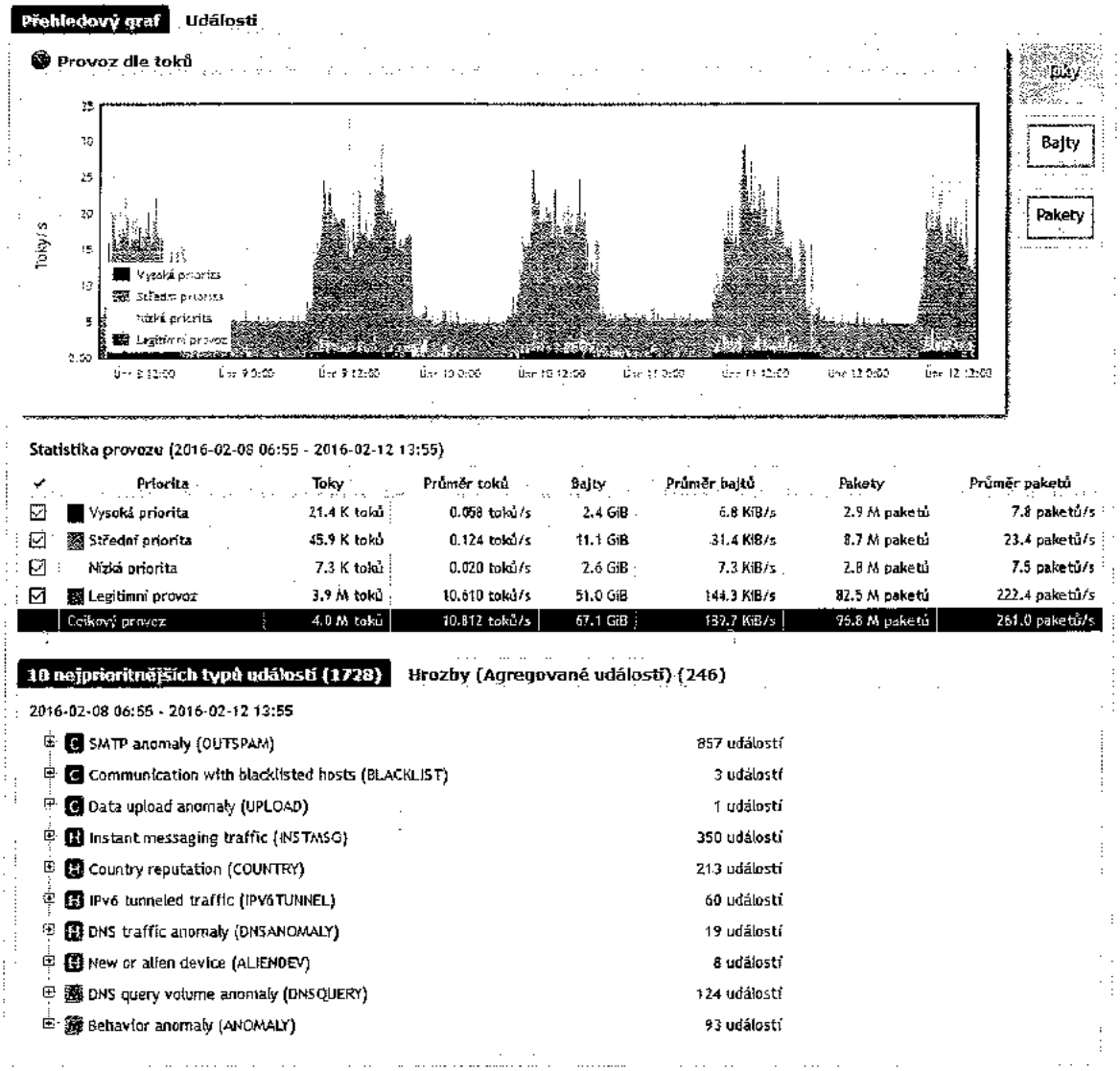


Popis zařízení - Licence na Flowmon ADS - FPC-ADS-C verze Corporate

Flowmon Anomaly Detection System (ADS) je vyspělé řešení pro odhalování provozních problémů a ochranu podnikových sítí před moderními kybernetickými hrozbami, které využívá technologii detekce anomálií a analýzy chování v síti (NBAD).

Na rozdíl od IDS systémů a SNMP monitoringu sleduje Flowmon ADS celkové chování zařízení v síti, díky čemuž umožňuje odhalovat a reagovat na doposud neznámé nebo specifické hrozby. A to včetně těch, pro které neexistuje signatura. Díky Flowmon ADS získávají administrátoři klíčovou výhodu v boji s moderními bezpečnostními hrozbami, které obchází tradiční ochranné prvky, jako jsou firewall, IDS/IPS systémy nebo antivirové programy. Toto řešení poskytuje vždy naprosto přesné informace o síťovém provozu, šetří náklady na její správu a posouvá zabezpečení firemní infrastruktury na novou úroveň

Flowmon ADS je dostupný jako softwarový modul pro Flowmon kolektor nebo Flowmon sondu. Jednoduchý instalační proces umožňuje mít plně funkční řešení pro analýzu chování sítě během několika minut. Veškeré metody detekce anomálií jsou dostupné tzv. out-of-box. Portfolio dostupných modelů Flowmon ADS plně vyhovuje potřebám menších, středních i velkých firem a organizací.



Popis zařízení - Flowmon Probe 4000 a Flowmon Probe 20000 SFP+

Flowmon sondy jsou základním předpokladem moderního monitorování síťové infrastruktury. Tato výkonná síťová zařízení poskytují administrátorům detailní statistiky o síťové komunikaci v podobě IP toků (standardy NetFlow v5/v9, IPFIX a další). Přináší tak naprosto přesné informace o tom, kdo komunikoval, s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další důležité informace z vrstev L2 - L4. Ty jsou nezbytné pro zajištění síťové bezpečnosti, řešení provozních problémů, účtování datových služeb, plánování kapacit linek, monitorování uživatelů/služeb a další cílové aplikace.

Flowmon sondy jsou pasivní zařízení, které nijak neovlivňují provoz sítě a překonávají omezení získávání NetFlow pomocí aktivních síťových prvků. Oproti jiným řešením navíc poskytují i viditelnost do aplikační vrstvy L7 a posouvají tak poznání toho, co se v síti děje, na úplně novou úroveň. Vedle výkonových parametrů sítě dovolují například sledovat HTTP/HTTPS aplikace z pohledu uživatele nebo výkonnost databází. Díky tomu lze řešit až 95 % provozních problémů ve vaší síti! Statistiky o provozu jsou Flowmon sondou exportovány ke zpracování na Flowmon kolektor či jinou kolektorovou aplikaci.

2.3 Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik

AddNet je unikátní DDI/NAC nástroj pro řádové zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích. Toho je dosaženo integrací systémů správy IP adresního prostoru, základních síťových služeb (DHCP, DNS), L2 monitoringu, řízení přístupu do sítě (NAC) a pokročilé komunikace s aktivními prvky sítě.

AddNet podporuje jednotné rozhraní pro správu IPAM s L2 monitoringem, DDI i NAC. V praxi tak operátoři ušetří mnoho času při správě zařízení, oproti běžné správě, kdy tyto činnosti znamenají operace prováděné ve více různých systémech. V AddNetu přidání nového zařízení do sítě znamená práci na 20 vteřin!

Integrovaný L2 monitor upozorní na nové/neznámé zařízení v síti, jednoznačně určí místo jeho v síti a případně rovněž jeho fyzickou lokalitu. Správce může následně, na jedné obrazovce, vybrat všechny potřebné informace, které mu AddNet nabízí a ty doplnit o potřebné unikátní informace. Na jedné obrazovce tak zadá nebo vybere a následně potvrdí informace o adresním plánování, vybrané síti, doby platnosti, začlenění do kritické infrastruktury, specifických DHCP voleb, DNS jménu apod. Po potvrzení záznamu dojde k okamžité distribuci informaci do celé AddNet infrastruktury a updatu všech klíčových subsystémů AddNetu (IPAM, DHCP, DNS, RADIUS).

AddNet pokrývá následující oblasti:

- Výkonný L2 monitoring
- Kompletní DDI (DHCP/DNS/IPAM)
- Integrovaný NAC
- Podpora krizového plánování
- Síťová správa a řízení přístupu pro BYOD a mobilní zařízení
- Pokročilá komunikace s aktivními prvky (SO - switch interoperability)
- Přehledový dashboard
- Výkonný reporting

AddNet není unikátní jenom rozsahem své funkcionality – L2 monitor/DDI/NAC. Přináší celý promyšlený komplex technologií, služeb a v neposlední řadě rovněž připravené integrace s návaznými systémy zvýšení užitné hodnoty v rámci ochrany a efektivní správy vnitřní sítě organizace. Součástí dodávky tak není pouze implementace DDI/NAC nástroje, ale rovněž komplexní přenos know-how pro vysoce efektivní IP správu a zabezpečení sítě organizace

Klíčové přínosy AddNetu

- Významná úspora práce síťových administrátorů
- Standardizace činností síťových správců a možnost centralizace správy rozsáhlých distribuovaných sítí
- Vysoce výkonný L2 monitoring s možností fyzické lokalizace zařízení – díky integraci s kabelovou knihu
- Podstatné zvýšení provozní spolehlivosti a výkonu základních síťových služeb sítě - DNS, DHCP, Radius
- Zavedení řízení bezpečnosti přístupu do sítě s využitím plného 802.1x nebo MAC autentizace s následnou autorizací (přiřazování do VLAN)

- Plně automatizovaná správa BYOD a mobilních zařízení
- Jednoznačná identifikace BYOD a mobilních zařízení v síti
- Nadstandardní škálovatelnost, zajištění funkcionality na pobočkových sítích i v případě nedostupnosti spojení s centrálou
- Úspora nákladů díky dlouhodobému sledování portové utilizace aktivních prvků
- Plná heterogennost a bezproblémová spolupráce se síťovými technologiemi Microsoft a Cisco

Nabízené řešení se stává z následujících součástí:

- AddNet Enterprise Server Edition – 5000 – 1ks
- AddNet Enterprise Server Edition HA – 5000 – 1ks
- AddNet Work server – 6ks
- AddNet Work server Branch office Edition – 100 – 12ks
- FireBox Add-on - Flowmon Exporter - 1Gbit/100 IPs – 12ks

Popis řešení – AddNet Enterprise Server Edition a HA edition

AddNet řídící server je centrální částí AddNetu. AddNet řídící servery slouží k poskytování webového uživatelského rozhraní pro síťové a bezpečnostní správce. Slouží jako primární zdroj konfigurace pro AddNet systém vzhledem k modelu sítě. Zároveň přijímá a zpracovává data z monitoringu, DHCP, DNS... od podřízených AddNet workserverů. Prezentuje je ve vysoce sofistikované podobě s ohledem na existující konfigurace a stav sítě.

Řídící servery je možné provozovat samostatně, v rámci aktivního clusteringu nebo v rámci hierarchie řídících serverů (pro velmi rozsáhlé organizace). V rámci toho řešení je nabízeno HA řešení.

Popis řešení - AddNet Work server a Branch office Edition

AddNet workserver je výkonnou částí AddNetu, která provozuje aktivní L2 monitoring a komunikuje s aktivními prvky. Získané informace v agregované formě zasílá AddNet řídícímu serveru (nebo nadřazeným řídícím serverům). Z těchto serverů naopak putují informace o aktuálních změnách konfigurace sítě a základních síťových služeb (DDI/NAC). AddNet workserver poskytuje také základní síťové služby (DHCP, DNS, a NTP) a služby NAC (RADIUS a NTP).).

Tyto služby mohou být konfigurovány v lokální nebo vzdálené redundanci (podpora vícenásobného clusteringu typu Active-Active). AddNet workserver dokáže zajistit kontinuitu provozu základních síťových služeb (DHCP/DNS/NTP) včetně NAC (Radius) a monitoringu i v sítích, které jsou dočasně odpojeny od centrální lokality. Dostupnost AddNet řídících serverů tak není pro kontinuitu provozu AddNetu nezbytná – projeví se pouze nedostupností aplikačního rozhraní pro možnost změny konfigurace sítě.

Branch office Edition slouží pro řešení OJ.

Popis řešení - FireBox Add-on - Flowmon Exporter - 1Gbit/100

Licence nahrazuje funkcionalitu Flowmon Sondy na vzdálených lokalitách, funkcionalita je stejná jako u Flowmon sondy.

2.4 Školení

- Uživatelské školení pro systém Monitoringu a vyhodnocování toků v síti (rozsah 1MD), počet účastníků až 20;
    - Základní školení pro administrátory, kteří budou schopni řešit základní incidenty v rámci Flowmon řešení
- Administrátorské školení pro systém Monitoring a vyhodnocování toků v síti (rozsah 3MD), počet účastníků až 4;
    - Pokročilé školení zaměřené na funkcionalitu modulu ADS.
- Uživatelské školení pro systém Monitoring sítě, správu adresního prostoru a systém řízení přístupových politik (rozsah 1MD), počet účastníků až 20;
    - Základní školení pro administrátory, kteří budou schopni řešit základní pracovní postupy při nasazení ADDNetu – obsluha systému a řešení provozních věcí.
- Administrátorské školení pro systém Monitoring sítě, správu adresního prostoru a systém řízení přístupových politik (rozsah 2MD), počet účastníků až 4.
    - Pokročilé školení zaměřené na nastavování nových funkcionalit, integraci s Flowmon řešením a řešení případných problémů.

Veškerá školení proběhnou v českém jazyce, budou prováděna certifikovaných specialistou a budou v místě specifikovaném zákazníkem (v České republice).

LESY ČR

Příloha č. 2: Ceník

Položka	Jednotek	Jednotková cena v Kč bez DPH	Celková cena v Kč bez DPH
Systém pro agregaci logů bezpečnostního řešení perimetru s podporu automatizace reportů a centrální správy zařízení perimetru			
Logovací a reportovací systém perimetru	1	*132 000*	*132 000*
Systém centrální správy perimetru	1	*530 000*	*530 000*
Systém pro monitoring a vyhodnocování toků v síti			
Kolektor s detekcí anomálií	1	*1 872 000*	*1 872 000*
1G Sonda	1	*195 000*	*195 000*
10G Sonda	1	*520 000*	*520 000*
Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik			
Centrální část řešení pro generální ředitelství a centrální datacentrum	1	*4 685 000*	*4 685 000*
Pobočková část řešení pro krajská ředitelství	12	*222 300*	*2 667 600*
Nabídková cena celkem	---	---	*10 601 600*

Součástí ceny za dodávku jednotlivých položek jsou i náklady na veškeré související služby dodání do místa plnění, instalace a implementace, školení, zajištění projektového řízení a poskytnutí záruky za jakost za poskytnuté plnění v délce dvou (2) roků.

Příloha č. 3 kupní smlouvy - Čestné prohlášení o seznamu členů odborného týmu uchazeče

Seznam členů realizačního týmu

1.	Projektový manažer:	Ing. Jan Šámal (*1977)
2.	Specialista pro roli Senior technik:	Ing et. Ing. Tomáš Zloch (*1985)
3.	Specialista pro roli Junior technik:	Ing. Josef Blahut (*1989)

Zkrácený profesní životopis

Ing. Jan Šámal (*1977)

Zaměstnavatel

Huatech a.s. Sídlo: Vyskočilova 741/3, Michle, 140 00 Praha 4, IČO: 03665496

Pozice v týmu pro realizaci veřejné zakázky

Projektový manažer

Kontaktní informace

Telefon: 736504015
Email: jan.samal@huatech.cz

Vzdělání

1995-2001 ČVUT v Praze, Fakulta elektrotechnická, inženýrský studijní program Telekomunikační technika, titul: Ing.

Pracovní zkušenosti

2015-dosud Huatech a.s. ... projektový manažer

2008-dosud OSVČ ... Poradenství v telekomunikacích a informačních technologiích – ICT konzultant, projektový manažer, technický dozor

2002-2007 OptiKom.cz, s.r.o. ... Interní technická podpora prodeje, analytik telekomunikačních řešení, ICT konzultant, technologický specialista na oblast LAN/WAN a hlasové infrastruktury, projektový manažer

2001-2002 SPŠ Sdělovací Techniky ... civilní služba – počítačový technik, LAN administrátor, ICT konzultant

2000-2001 TELECOMSPOL, spol. s r.o. ... Interní technická podpora obchodu, technik, inženýr speciálních projektů

Certifikace

12/2015 Huawei Sales Specialist – IP Network
(HCS-IP-Sales: 030120001240806062931409)
Huawei Sales Specialist – Information Technology
(HCS-IT-Sales: 030120201240806062971409)

10/2014 PRINCE2 Introduction

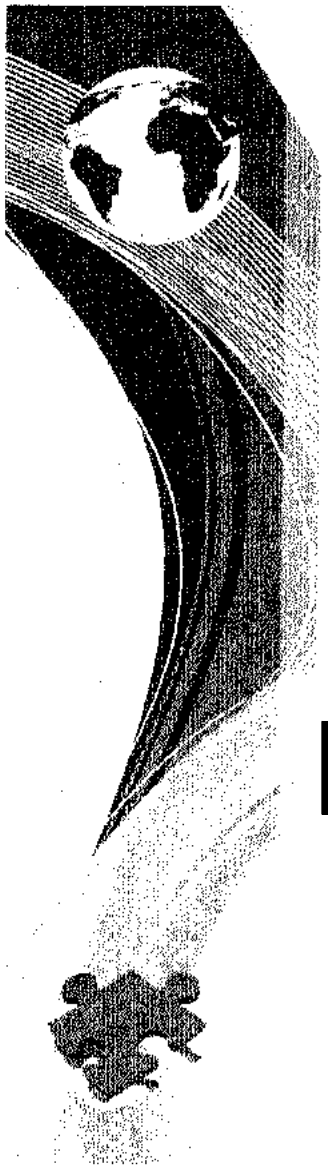
3/2012 ITIL v3 Foundation – Information Technology Infrastructure Library

Vybrané realizované projekty

2015 Bank of China, Prague branch – projekt „Implementace ICT řešení (LAN, WLAN, hostovaná IP telefonie, UC&C) pražské pobočky BoC"; pozice: projektový manažer; hodnota realizovaného projektu: 2 mil Kč bez DPH

2011-2012 Povodí Moravy s.p. – „Implementace ICT technologií (LAN, IP telefonie, network security) v prostředí sítě LAN/WAN POMO a datového centra POMO"; pozice: projektový manažer, technický dozor investora, ICT konzultant; hodnota realizovaného projektu: 8 mil Kč bez DPH

2009-2010 Statutární město Ústí nad Labem – „Implementace ICT technologií (LAN, IP telefonie) v prostředí rozsáhlé metropolitní sítě města Ústí nad Labem"; pozice: projektový manažer a technický dozor investora, ICT konzultant; hodnota realizovaného projektu: 8 mil Kč bez DPH



tayllorcox.com
Please your certification

PRINCE2® Intro

TAYLLOR & COX Global Ltd. confirms, that Project Manager

Mr. JAN SAMAL

has successfully completed the accredited course of PRINCE2® Intro
Course date: 27. 10. 2014

[redacted]
Chief Executive

Certificate No: PCE 14 P2i 2615

TAYLLOR & COX is RCB - Registered Certification Bodies & ATO - Accredited Training Organisation & Examination Center for PRINCE2® by Project Management, ITIL® by IT Infrastructure Library, ITSM® by IT Service Management, MSP® by Managing Successful Programmes, TOGAF® by The Open Group Architecture Framework, ISMS® by Information Security Management, RISK® by Management of Risk & SAP®. Headoffice: TAYLLORCOX GLOBAL LIMITED; 3 PARKLANDS PLACE; GUILDFORD; SURREY; GU1 2PS; UNITED KINGDOM info@tayllorcox.com

This is to certify that

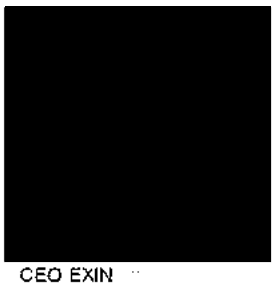
Jan Samal

has passed the

ITIL® version 3

Foundation Examination

19 March 2012



CEO EXIN

4453149.1084263

EXIN
The global certification company for Information Management

ITIL®

APM GROUP

OGC

00280009

ČESKÁ REPUBLIKA

Vysoká škola **ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**

Fakulta elektrotechnická

Číslo diplomu 000173 Č. 85/2001

VYSOKOŠKOLSKÝ DIPLOM

Jan Šámal

(jméno a příjmení)

narozen(a) dne [redacted] v **Praze** okres **Praha**

ykonáním státní závěrečné zkoušky a získal(a) vysokoškolské vzdělání v magisterském studijním programu

elektrotechnika a informatika (2612T)

studijní obor **Telekomunikační technika**

Podle § 46 odst. 4 písm. a) zákona č. 111/1998 Sb. o vysokých školách se mu (jí) uděluje akademický titul

inženýr

ve zkratce **Ing.**

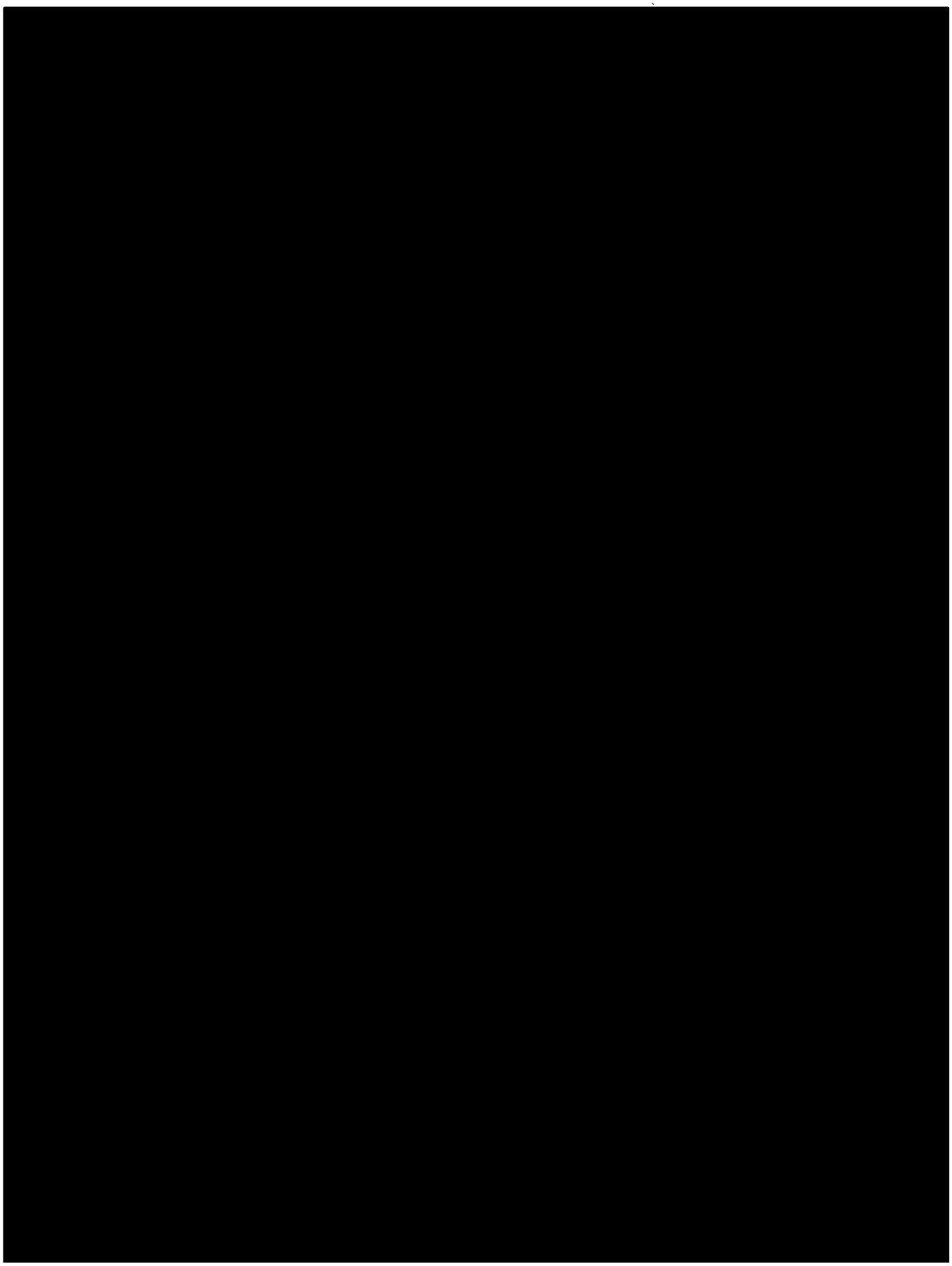
V Praze dne **21. března 2001**

..... [redacted] .....

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE L.S.

[redacted]

VSP/3327/R



Flowmon
Networks

hereby certifies

Tomáš Zloch

as an authorized

Flowmon

Technical Specialist

Successful completion of the training course

Network Performance Monitoring and Diagnostics

Issue Date: 07.12.2016

The certificate is valid for 2 years.

Flowmon Networks a. s., U Vodárny 2965/2, 616 00, Brno, Czech Republic
www.flowmon.com, info@flowmon.com

Flowmon
Networks

hereby certifies

Tomáš Zloch

as an authorized

Flowmon

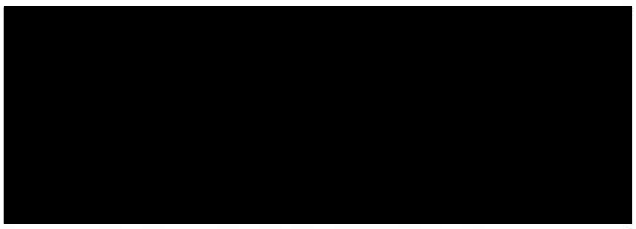
Technical Specialist

Successful completion of the training course

Flowmon Security

Issue Date: 14.12.2016

The certificate is valid for 2 years.



Flowmon Networks a. s., U Vodárny 2965/2, 616 00, Brno, Czech Republic
www.flowmon.com, info@flowmon.com

HUAWEI

Huawei Career Certification

Tomas Zloch

HAS SUCCESSFULLY COMPLETED THE HUAWEI CAREER CERTIFICATION REQUIREMENTS AND IS AUTHORISED AS A

Huawei Certified Network Professional

Valid Through Feb 04, 2019

Certificate ID: 010200101240806422251409

ČESKÁ REPUBLIKA
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

VYSOKOŠKOLSKÝ DIPLOM

Číslo diplomu: 10FELM0058

Tomáš Zloch
(jméno, příjmení)

[redacted]

získal vysokoškolské vzdělání studiem

v magisterském studijním programu **Elektrotechnika a informatika (N2612)**
ve studijním oboru **Telekomunikace a radiotechnika (2601T014)**

na Fakultě elektrotechnické.

Podle §46 odst. 4) zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), se mu uděluje akademický titul

inženýr
ve zkratce **Ing.**

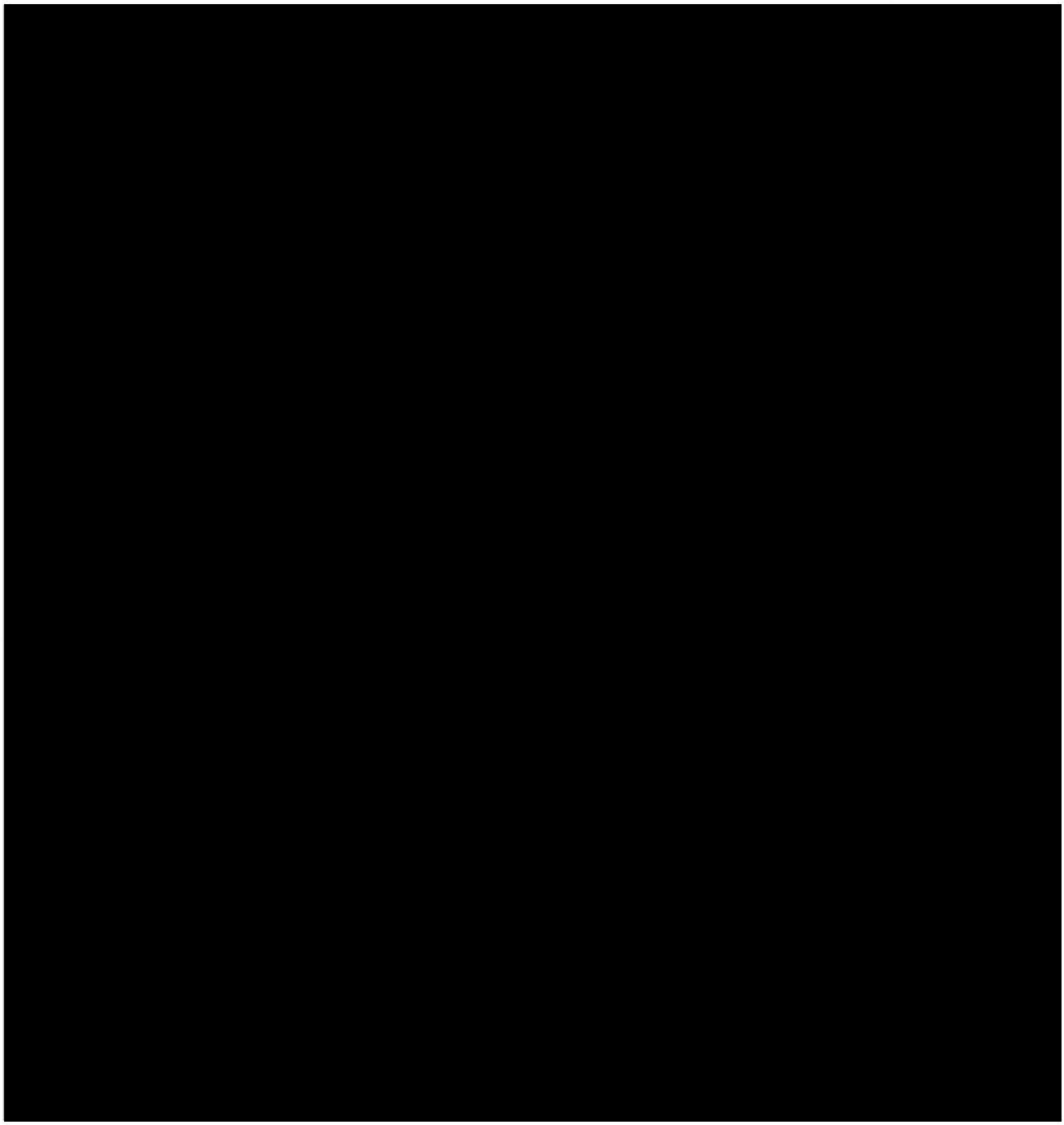
V Praze dne 26. l[redacted]

pro[redacted]

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

[redacted]
děkan fakulty

Zkrácený profesní životopis



Flowmon
Networks

hereby certifies

Josef Blahut

as an authorized

FlowMon Networks Consultant

T [redacted]

P [redacted]

FlowMon Networks, a. s., U Vodárny 2965/2, 616 00, Brno, Czech Republic
www.flowmon.com, info@flowmon.com

HUAWEI

Huawei Career Certification

Josef Blahut

HAS SUCCESSFULLY COMPLETED THE HUAWEI CAREER CERTIFICATION REQUIREMENTS AND IS AUTHORISED AS A

Huawei Certified Network Professional

Career Certification
HUAWEI
HCNP
Routing & Switching

Valid Through Feb 27, 2019
Certificate ID: 010200101458064232114O9

[redacted]

ČESKÁ REPUBLIKA
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

VYSOKOŠKOLSKÝ DIPLOM

Číslo diplomu: 16FELM0001

Josef Blahut
(jméno, příjmení)

[redacted]

získal vysokoškolské vzdělání studiem

v magisterském studijním programu **Komunikace, multimédia a elektronika (N2653)**
ve studijním oboru **Sítě elektronických komunikací (2612T069)**

na Fakultě elektrotechnické.

Studium bylo řádně ukončeno státní závěrečnou zkouškou dne 2. února 2016.
Podle §46 odst. 4) zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), se mu uděluje akademický titul

Inženýr
ve zkratce **Ing.**

[redacted]

L.S.

[redacted]

Příloha č. 4 kupní smlouvy – Harmonogram

Dodavatel uvede detailní závazný harmonogram realizace

Harmonogram musí reflektovat následující minimální požadavky zadavatele:

- *Předmět koupě (pro všechna místa plnění) bude dodán nejpozději do 2 měsíců od nabytí účinnosti kupní smlouvy;*
- *Předmět koupě (pro všechna místa plnění) bude nainstalován a implementován nejpozději do 3 měsíců od nabytí účinnosti kupní smlouvy;*
- *Školení pracovníků zadavatele proběhnou nejpozději do 3 měsíců od nabytí účinnosti kupní smlouvy.*

Detailnější členění harmonogramu dle konkrétních komponent nabízeného systému a dle jednotlivých míst plnění je plně v dikci dodavatele podávajícího nabídku.

nabytí účinnosti kupní smlouvy (den 0)	týden 1	týden 2	týden 3	týden 4	týden 5	týden 6	týden 7	týden 8	týden 9	týden 10	týden 11	týden 12
příprava instalace												
dodání předmětu koupě												
instalace v místě plnění												
školení prac. zadavatele												

- Harmonogram je platný při maximální součinnosti objednatele