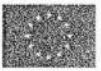

MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

Smlouva o dílo na realizaci akce

Kybernetická bezpečnost Krajského úřadu Olomouckého kraje
Implementace bezpečnostního projektu

I. SMLUVNÍ STRANY

1. Objednatel

Olomoucký kraj

zastoupený:	Ladislavem Oklešťkem, hejtmanem
se sídlem:	Olomouc, Hodolany, Jeremenkova 1191/40a
IČO:	60609460
DIČ:	CZ60609460
plátce DPH:	ANO
bankovní spojení (číslo účtu):	[redacted]

(dále jen „***Objednatel***")

a

2. Zhotovitel

MERIT GROUP a.s.

zastoupená:	Petrem Weigelem, statutárním ředitelem
se sídlem:	Březinova 136/7, Hodolany, 779 00 Olomouc
IČO:	64609995
DIČ:	CZ699000785
plátce DPH:	ano
zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě pod sp. zn. B 1221	
bankovní spojení (číslo účtu):	Československá obchodní banka, a. s., č.ú.: [redacted]
telefon:	[redacted]
e-mail:	[redacted]

(dále jen „***Zhotovitel***")

(Objednatel a Zhotovitel společně dále také jako „***Smluvní strany***")

uzavřeli v souladu s § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „***Občanský zákoník***"), tuto smlouvu o dílo (dále jen „***Smlouva***").

II. ÚVODNÍ UJEDNÁNÍ

3. Smlouva je uzavřena na základě výsledků zadávacího řízení (dále jen „***Řízení veřejné zakázky***") veřejné zakázky s názvem: **Kybernetická bezpečnost Krajského úřadu Olomouckého kraje II**, sp. zn. zadavatele: **OKKB0319** (dále jen „***Veřejná zakázka***"). Jednotlivá ujednání Smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky a nabídkou Zhotovitele podanou na Veřejnou zakázku. Nabídka Zhotovitele podaná do Řízení veřejné zakázky je pro Zhotovitele závazná.

4. Dílo podle Smlouvy je realizováno v rámci projektu „Kybernetická bezpečnost Krajského úřadu Olomouckého kraje", registrační číslo projektu CZ.06.3.05/0.0/0.0/15_011/0005028 (dále také „**Projekt**"), který je spolufinancován z Integrovaného regionálního operačního programu (dále jen „**Operační program**").

5. Zhotovitel je povinen při plnění povinností vyplývajících ze Smlouvy dodržovat požadavky stanovené podmínkami pro poskytnutí dotace z Operačního programu.

III. PŘEDMĚT SMLOUVY

6. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí ve sjednaném termínu pro Objednatele dále specifikované dílo: **zvýšení úrovně zabezpečení LAN sítě Objednatele a provozovaných služeb** (dále jen „***Dílo***").

7. Objednatel se zavazuje dokončené Dílo převzít a zaplatit za něj sjednanou cenu a příslušnou DPH, je-li Zhotovitel povinen podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***ZoDPH***") hradit DPH.

IV. PŘEDMĚT DÍLA

8. Zhotovitel se zavazuje provést pro Objednatele Dílo, jež sestává z těchto základních částí:
   8.1. implementace Web aplikačního firewallu (dále jen „**První etapa**");
   8.2. implementace Webové proxy (dále jen „**Druhá etapa**");
   8.3. implementace Next Generation IPS/Firewallu (dále jen „**Třetí etapa**");
   8.4. implementace systému pro řízení přístupu do komunikační infrastruktury úřadu (dále jen „**Čtvrtá etapa**");
   8.5. implementace Mobile Device Management systému (dále jen „**Pátá etapa**");
   8.6. penetrační testy;

   a to včetně všech souvisejících prací, dodávek a služeb. První až Pátá etapa budou dále označovány společně jako „**etapy Díla**", případně dle smyslu jednotlivě jako „**etapa Díla**".

9. Dílo je blíže vymezeno v přílohách č. 1 – 7 této Smlouvy, které obsahují zejm. funkční specifikaci jednotlivých etap Díla, rozdělení etap Díla na části, a podrobnější specifikaci plnění Zhotovitele.

10. Součástí Díla je rovněž následující plnění související s publicitou Projektu:
    10.1. výroba, osazení a následná demontáž informačního billboardu o rozměru 2,1 x 2,2 m po dobu realizace Díla na místě určeném Objednatelem,
    10.2. výroba a osazení pamětní desky o rozměru 0,3 x 0,4 m vyrobené z odolného a trvalého materiálu na místě určeném Objednatelem nejpozději současně s dokončením Díla dle čl. VII odst. 40 Smlouvy.

    Grafický návrh informačního billboardu a pamětní desky dodá Zhotoviteli Objednatel.

11. V rámci jednotlivých etap Díla a v rámci penetračních testů je Zhotovitel povinen poskytnout plnění dle příslušných příloh této Smlouvy, přičemž poskytnuté plnění musí splňovat všechny požadavky Objednatele v příslušné příloze uvedené nebo z jejího obsahu vyplývající. Zhotovitelem poskytnuté plnění musí odpovídat též všem návrhům řešení specifikovaným v nabídce Zhotovitele podané na Veřejnou zakázku.

12. Informativním podkladem pro provedení Díla je Studie proveditelnosti pro projekt „Kybernetická bezpečnost Krajského úřadu Olomouckého kraje" a dokument s názvem „Ověření účinnosti zavedených bezpečnostních opatření Olomouckého kraje vůči zákonu č. 181/2014 Sb. o kybernetické bezpečnosti", které jsou přílohou dokumentace zadávacího řízení Veřejné zakázky.

13. Dílo bude sloužit k účelu vyplývajícímu z dokumentů uvedených v předchozím odstavci, který lze zjednodušeně vyjádřit jako zvýšení úrovně zabezpečení LAN sítě Objednatele a provozovaných služeb.

14. Zhotovitel je povinen při provádění Díla provést, dodat a poskytnout veškeré práce, dodávky a služby, kterých je třeba trvale nebo dočasně k zahájení, provádění, dokončení a předání Díla, a provozování LAN sítě Objednatele a provozovaných služeb s vyšší úrovní zabezpečení zajištěnou splněním této Smlouvy.

15. Rozsah a kvalita Díla jsou dále dány příslušnými ČSN, ČSN EN, českými i evropskými právními předpisy platnými a účinnými v době provádění Díla, a dalšími podmínkami sjednanými ve Smlouvě.

16. Zhotovitel je povinen zajistit veškeré nezbytné doklady, prohlídky a přejímky, spojené s prováděním Díla, vyžadované Smlouvou, českými či evropskými právními předpisy nebo orgány veřejné správy.

17. Zhotovitel prohlašuje, že se před podpisem Smlouvy seznámil s předmětem Díla a místem plnění, a že s ohledem na své znalosti a zkušenosti zhotoví Dílo tak, aby mohlo být řádně užíváno k účelu, k němuž má být provedeno, přičemž si není vědom žádných překážek, které by mu bránily v poskytnutí sjednaného plnění v souladu se Smlouvou.

18. Zhotovitel je při určení způsobu provádění Díla vázán příkazy Objednatele, pokud Objednatel Zhotoviteli takové příkazy udělí.

19. Změny Díla, včetně provedení veškerých víceprací, méněprací, změny technologií nebo materiálů, doplňky, rozšíření či zúžení Díla, je možné činit pouze za podmínek stanovených zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen ***„Zákon o zadávání veřejných zakázek"***), a musí být vždy sjednány předem ve formě písemného dodatku ke Smlouvě, nestanoví-li Smlouva jinak. Nebude-li písemný dodatek obsahovat ujednání o důsledcích sjednaných změn na výši sjednané ceny Díla, je Objednatel povinen bez ohledu na sjednané změny Díla zaplatit cenu Díla sjednanou ve Smlouvě.

V. CENA

20. Cena za provedení Díla činí **23 145 930,00 Kč bez DPH** (dále jen ***„Cena Díla"***); DPH činí **4 860 645,30 Kč; Cena Díla včetně DPH** činí **28 006 575,30 Kč.** Cena Díla je podrobně rozčleněna v položkovém rozpočtu, který tvoří přílohu č. 8 Smlouvy (dále jen ***„Položkový rozpočet"***).

21. Cena Díla je stanovena jako pevná, nejvýše přípustná a nepřekročitelná s výjimkami sjednanými ve Smlouvě. Cena Díla zahrnuje zisk Zhotovitele a veškeré náklady, které Zhotovitel v rámci plnění Smlouvy vynaloží.

22. Vyskytne-li se při provádění Díla potřeba provést vícepráce, je Zhotovitel povinen provést bez zbytečného odkladu přesný soupis všech víceprací, které je nutné provést, včetně jejich ocenění s ohledem na počet měrných jednotek a jednotkové ceny dle Položkového rozpočtu, a tento soupis předložit Objednateli ke schválení. Je-li nezbytné provést práce, dodávky či služby v Položkovém rozpočtu neobsažené nebo neoceněné, je Zhotovitel povinen provést jejich ocenění tak, aby nepřevyšovalo cenu v daném místě a čase obvyklou. Objednatel je povinen vyjádřit se k podle předchozí věty Zhotovitelem navrženému soupisu víceprací nejpozději do 5 pracovních dnů ode dne jeho předložení Zhotovitelem Objednateli. Bude-li navržený soupis víceprací Objednatelem schválen, provedou Smluvní strany změnu rozsahu Díla a Ceny Díla podle schváleného soupisu víceprací formou dodatku ke Smlouvě v souladu s platnými právními předpisy. Zhotovitel není oprávněn požadovat zvýšení Ceny Díla, jestliže přesný soupis víceprací včetně jejich ocenění s ohledem na počet měrných jednotek a jednotkové ceny nepředloží Objednateli ke schválení bez zbytečného odkladu poté, kdy se zvýšení Ceny Díla ukázalo jako nevyhnutelné.

23. Po výpočtu změny Ceny Díla vyhotoví Zhotovitel písemný návrh dodatku ke Smlouvě, jehož obsahem bude zejména rozsah změn Díla, změna Ceny Díla včetně detailního položkového rozpočtu a vliv této změny na termíny plnění podle Smlouvy. V případě, že vliv na termíny plnění podle Smlouvy nebude v návrhu dodatku uveden, termíny plnění podle Smlouvy zůstávají beze změny.

24. Objednatel je povinen zaplatit Zhotoviteli a Zhotovitel je oprávněn Objednateli vyúčtovat pouze Cenu Díla podle Zhotovitelem skutečně provedených dodávek a služeb (činností). Neprovede-li Zhotovitel některé dodávky nebo služby (činnosti) dle Položkového rozpočtu nebo jejich část, sníží se Cena Díla o hodnotu neposkytnutých dodávek nebo služeb (činností).

25. Smluvní strany se dohodly, že § 2620, § 2621 a § 2622 Občanského zákoníku a rovněž obchodní zvyklosti, jež jsou svým smyslem nebo účinky stejné nebo obdobné uvedeným ustanovením, se nepoužijí.

VI. FAKTURACE A PLATEBNÍ PODMÍNKY

26. Je-li Zhotovitel povinen podle ZoDPH uhradit v souvislosti s poskytováním plnění podle Smlouvy DPH a Dílo nepodléhá režimu přenesení daňové povinnosti dle ZoDPH, je Objednatel povinen Zhotoviteli takovou DPH uhradit vedle Ceny Díla. Zhotovitel odpovídá za to, že sazba DPH bude ve vztahu ke všem plněním poskytovaným na základě Smlouvy stanovena v souladu s právními předpisy platnými a účinnými k okamžiku uskutečnění zdanitelného plnění.

27. Objednatel bude hradit Zhotoviteli Cenu Díla na základě faktur (dále jen „***Faktura***"), vystavených za práce, dodávky a služby na Díle provedené, dodané a poskytnuté v rámci každé etapy Díla vždy po dokončení každé jednotlivé etapy Díla. Datum uskutečnění zdanitelného plnění se shoduje s datem dokončení příslušné etapy Díla dle odst. 41 Smlouvy, za kterou je Faktura vystavována. Po převzetí Díla Objednatelem v souladu se Smlouvou vystaví Zhotovitel závěrečnou Fakturu (dále jen „***Závěrečná Faktura***") vystavenou za práce, dodávky a služby na Díle provedené, dodané a poskytnuté od poslední vystavené Faktury do převzetí Díla Objednatelem. Datum uskutečnění zdanitelného plnění u Závěrečné Faktury je den převzetí Díla Objednatelem.

28. Faktura musí splňovat náležitosti daňového dokladu podle ZoDPH, včetně případné informace, že provedení Díla podléhá režimu přenesení daňové povinnosti dle ZoDPH. V případě, že Zhotovitel není plátcem DPH, musí Faktura splňovat náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. Faktura musí vždy splňovat náležitosti stanovené § 435 Občanského zákoníku. Faktura musí dále odpovídat požadavkům stanoveným podmínkami pro poskytnutí dotace z Operačního programu, musí obsahovat zejm. název Projektu „Kybernetická bezpečnost Krajského úřadu Olomouckého kraje" a registrační číslo Projektu CZ.06.3.05/0.0/0.0/15_011/0005028. Zhotovitel je povinen použít na Faktuře bankovní účet zveřejněný v registru plátců podle § 96 ZoDPH.

29. Zhotovitel je povinen předložit Objednateli před vystavením každé Faktury soupis provedených, dodaných a poskytnutých prací, dodávek a služeb oceněných v souladu s Položkovým rozpočtem (dále jen ***„Soupis"***). Soupis bude obsahovat rozsah všech prací, dodávek a služeb provedených, dodaných a poskytnutých při provádění Díla za příslušnou etapu Díla, za kterou bude Faktura vystavena. Zhotovitel je povinen předložit Soupis Objednateli před vystavením Faktury k odsouhlasení, a to do 5 pracovních dnů od data uskutečnění zdanitelného plnění, a Faktura může být vystavena až po odsouhlasení Soupisu Objednatelem.

30. Objednatel je povinen se k Soupisu vyjádřit nejpozději do 5 pracovních dnů ode dne jeho obdržení. Vyjádří-li Objednatel se Soupisem nesouhlas, projednají Smluvní strany výhrady Objednatele k Soupisu a Zhotovitel poté předloží Objednateli k odsouhlasení opravený Soupis.

31. Zhotovitel vystaví Fakturu nejpozději do 5 pracovních dnů ode dne odsouhlasení Soupisu Objednatelem. Nedílnou součástí Faktury musí být Soupis podepsaný Objednatelem.

32. Z důvodu předfinancování Projektu z revolvingového úvěru vedeného u Komerční banky a.s., musí být do nejbližší možné Rady Olomouckého kraje (dále jen „**ROK**") předloženy jednotlivé Faktury k úhradě a souběžně také předložena žádost o zapojení finanční prostředků z revolvingového úvěru na úhradu těchto Faktur dle zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů. Jelikož termíny ROK jsou stanoveny 2x do kalendářního měsíce, sjednává se lhůta splatnosti Faktury v délce 60 dnů ode dne doručení Faktury Objednateli.

33. Stanoví-li Faktura splatnost delší, než je jako minimální stanovena v tomto článku, je Objednatel oprávněn uhradit Cenu Díla, případně její část, a případnou DPH ve lhůtě splatnosti určené ve Faktuře.

34. Cena Díla, případně její část, vyúčtovaná Fakturou a případná DPH je uhrazena vždy dnem jejich odepsání z bankovního účtu Objednatele.

35. Objednatel si vyhrazuje právo uplatnit institut zvláštního způsobu zajištění daně z přidané hodnoty ve smyslu § 109a ZoDPH, pokud Zhotovitel bude požadovat úhradu za zdanitelné plnění na bankovní účet, který nebude nejpozději ke dni splatnosti příslušné Faktury zveřejněn správcem daně v příslušném registru plátců daně (tj. způsobem umožňujícím dálkový přístup). Obdobný postup je Objednatel oprávněn uplatnit i v případě, že v okamžiku uskutečnění zdanitelného plnění bude o Zhotoviteli zveřejněna v příslušném registru plátců daně skutečnost, že je nespolehlivým plátcem nebo v případě naplnění dalších kritérií uvedených v § 109 odstavci 1 a 2 ZoDPH. V případě, že nastanou okolnosti umožňující Objednateli uplatnit zvláštní způsob zajištění daně podle § 109a ZoDPH, bude Objednatel o této skutečnosti Zhotovitele informovat. Při použití zvláštního způsobu zajištění daně bude příslušná výše DPH zaplacena na účet Zhotovitele vedený u jeho místně příslušného správce daně, a to v původním termínu splatnosti. V případě, že Objednatel institut zvláštního způsobu zajištění daně z přidané hodnoty ve shodě s tímto ujednáním uplatní, a zaplatí částku odpovídající výši daně z přidané hodnoty uvedené na

daňovém dokladu vystaveném Zhotovitelem na účet Zhotovitele vedený u jeho místně příslušného správce daně, bude tato úhrada považována za splnění části závazku Objednatele odpovídajícího příslušné výši DPH, kterou je povinen dle Smlouvy uhradit vedle Ceny Díla.

36. Nebude-li příslušná Faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně stanovena Cena Díla či její část, DPH nebo jiná náležitost Faktury, je Objednatel oprávněn tuto Fakturu vrátit Zhotoviteli k provedení opravy s vyznačením důvodu vrácení. Zhotovitel je povinen opravit Fakturu podle pokynů Objednatele a opravenou Fakturu neprodleně doručit Objednateli.

37. Objednatel neposkytuje Zhotoviteli žádné zálohy.

VII. MÍSTO A TERMÍNY PLNĚNÍ

38. Místem plnění je sídlo Objednatele.

39. Zhotovitel je povinen Dílo provést (dokončit a předat Objednateli) do 5 měsíců ode dne nabytí účinnosti této Smlouvy.

40. Dokončením Díla se rozumí
    40.1. úspěšné dokončení všech pěti etap Díla,
    40.2. úspěšné dokončení penetračních testů,
    40.3. předání Předávací dokumentace (viz přílohy č. 1 – 5 Smlouvy) k jednotlivým etapám Díla Objednateli,
    40.4. splnění všech povinností Zhotovitele dle Smlouvy souvisejících s publicitou Projektu.

41. Úspěšným dokončením etapy Díla se rozumí úspěšné dokončení všech jednotlivých částí etapy Díla. Úspěšným dokončením jednotlivé části etapy Díla se rozumí podpis akceptačního protokolu k příslušné části etapy Díla oběma Smluvními stranami s výrokem „splňuje". Úspěšným dokončením penetračních testů se rozumí podpis akceptačního protokolu k penetračním testům oběma Smluvními stranami s výrokem „splňuje".

42. Zhotovitel je povinen zajistit úspěšné dokončení všech jednotlivých částí všech etap Díla v termínech uvedených v Harmonogramu, který je přílohou č. 9 této Smlouvy. Jednotlivé etapy Díla mohou být prováděny zároveň, není nezbytné, aby na sebe navazovaly v pořadí dle svého názvu. Jednotlivé části jednotlivé etapy Díla musejí být prováděny chronologicky dle svého číselného označení.

43. Zhotovitel je povinen upozornit Objednatele bez zbytečného odkladu na nevhodnou povahu nebo neúplnost věci nebo podkladu, které mu Objednatel předal k provedení Díla, nebo na nevhodnou povahu nebo neúplnost příkazu, který mu Objednatel dal. Jestliže nevhodné nebo neúplné věci, podklady nebo příkazy Objednatele překážejí v řádném provádění Díla, Zhotovitel v nezbytném rozsahu přeruší provádění Díla do doby výměny nebo doplnění věcí nebo podkladů nebo změny příkazů Objednatelem, nebo do doby doručení písemného sdělení Objednatele, že trvá na provádění Díla s použitím předaných věcí nebo podkladů nebo na dodržování jeho příkazů. Zhotovitel je povinen pokračovat v provádění Díla v rozsahu, ve kterém mu v tom nebrání nevhodné nebo neúplné věci, podklady nebo příkazy a technologický postup provádění Díla. Termíny plnění dle Smlouvy, byly-li přerušením provádění Díla přímo dotčeny, se prodlužují o dobu přerušením vyvolanou.

44. Zjistí-li Zhotovitel v průběhu provádění Díla, že nelze dodržet termíny dle Smlouvy, je povinen vždy na to Objednatele bez zbytečného odkladu upozornit. Tím nejsou dotčeny další povinnosti

Zhotovitele, zejména povinnost zaplatit smluvní pokutu za prodlení s plněním Díla a odpovědnost Zhotovitele za způsobenou újmu.

45. Termíny plnění dle Smlouvy mohou být změněny pouze písemným dodatkem ke Smlouvě.

VIII. PODMÍNKY PLNĚNÍ PŘEDMĚTU SMLOUVY

46. Zhotovitel je oprávněn provádět Dílo v sídle Objednatele v pracovní dny takto: v PO a ST od 7 do 17 hod.; v ÚT od 7 do 16 hod.; ve ČT od 7 do 15 hod. a v PÁ od 7 do 14 hod. Mimo uvedenou dobu je Zhotovitel oprávněn provádět Dílo v sídle Objednatele pouze po dohodě s Objednatelem. Objednatel je oprávněn v případě svých provozních potřeb dobu, po kterou je Zhotovitel oprávněn provádět Dílo, upravit písemným pokynem Zhotoviteli.

47. Je-li k provedení Díla nutná součinnost Objednatele, Zhotovitel informuje Objednatele o rozsahu a formě požadované součinnosti alespoň 1 (jeden) pracovní den předem a určí mu přiměřenou lhůtu k jejímu poskytnutí. Neposkytne-li Objednatel Zhotoviteli požadovanou součinnost, ačkoliv byl o potřebě poskytnutí součinnosti Zhotovitelem včas informován a byla mu k poskytnutí součinnost Zhotovitelem dána přiměřená doba, postupuje se přiměřeně podle odstavce 43 Smlouvy. Zhotovitel není oprávněn odstoupit od Smlouvy z důvodu neposkytnutí součinnosti Objednatelem.

48. Veškeré testy Díla, které je Zhotovitel povinen dle Smlouvy připravit, je před provedením testů povinen předat Objednateli k odsouhlasení. Objednatel je povinen vyjádřit se k návrhu testu nejpozději do 5 pracovních dnů od doručení návrhu testu Objednateli. Vyjádří-li Objednatel v uvedené době nesouhlas s návrhem testu, je Zhotovitel povinen návrh testu upravit dle připomínek Objednatele, které Objednatel zašle společně s nesouhlasem. Po provedení úpravy návrhu testu dle připomínek Objednatele zašle Zhotovitel upravený návrh testu Objednateli ke schválení. V případě potřeby se celý postup opakuje do doby vyslovení souhlasu Objednatele s návrhem testu. Komunikace mezi Smluvními stranami dle tohoto odstavce může probíhat elektronicky bez užití služeb nebo prostředků vytvářejících důvěru (tedy např. prostou emailovou komunikací bez využití zaručeného elektronického podpisu).

49. Proškolení zástupců Objednatele v rámci provádění jednotlivých etap Díla provede Zhotovitel v rozsahu přiměřeném příslušné etapě Díla. Zhotovitel provede celkem 5 proškolení (pro každou etapu Díla jedno), vždy pro cca 5 – 6 zástupců Objednatele. Jednotlivá proškolení se nesmí časově překrývat, neboť jeden zástupce Objednatele se může zúčastnit více školení.

50. Zhotovitel bere na vědomí, že plnění dle Smlouvy bude poskytovat v rámci Významných informačních systémů, jejichž správcem je Objednatel. S ohledem na uvedené je Zhotovitel povinen poskytovat plnění dle Smlouvy zejm. v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), resp. tak, aby se Zhotovitel vyvaroval jakékoliv činnosti, jež by mohla být označena za porušení uvedených právních předpisů Objednatelem.

51. Zhotovitel je povinen zachovat bezpečnost informací a dat obsažených ve Významných informačních systémech spravovaných Objednatelem, včetně jiných informačních systémů, kterou budou plněním Smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Plnění dle Smlouvy je Zhotovitel povinen poskytovat tak, aby důvěrnost, dostupnost a integrita informací a dat dle předchozí věty nebyla přerušena, ohrožena, ani omezena. Je-li

k plnění dle Smlouvy nezbytné důvěrnost, dostupnost či integritu dat omezit, ohrozit nebo přerušit, může tak Zhotovitel učinit pouze po předchozím souhlasu Objednatele a jen v rozsahu Objednatelem předem odsouhlaseném.

52. Zhotovitel není oprávněn užít informace ani data obsažená ve Významných informačních systémech spravovaných Objednatelem, ani v jiných informačních systémech, kterou budou plněním Smlouvy dotčeny. Je-li užití informací či dat dle předchozí věty nezbytné k plnění dle Smlouvy, může je Objednatel využít jen po předchozím souhlasu Objednatele a jen v rozsahu Objednatelem předem odsouhlaseném.

53. Objednatel je oprávněn kontrolovat kdykoliv a jakýmkoliv způsobem, zda Zhotovitel řádně plní veškeré povinnosti, které Zhotoviteli ze Smlouvy vyplývají. Objednatel je oprávněn kontrolu provádět i v provozovnách Zhotovitele a na jiných místech, kde Zhotovitel provádí činnosti, které souvisí s činností Zhotovitele dle Smlouvy. Zhotovitel je povinen poskytnout Objednateli ke kontrole dle tohoto odstavce potřebnou součinnost.

54. Zhotovitel je povinen dodržovat veškeré bezpečnostní politiky Objednatele. Objednatel je povinen před zahájením plnění dle této Smlouvy Zhotovitele seznámit s bezpečnostní politikou Objednatele. O seznámení Zhotovitele s bezpečnostní politikou Objednatele bude vyhotoven zápis.

55. Zhotovitel je povinen v průběhu plnění této Smlouvy průběžně spolupracovat s garantem aktiva Objednatele za účelem identifikace významných změn a jejich dopadů do oblasti kybernetické bezpečnosti Objednatele v souladu s § 11 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci (vyhláška o kybernetické bezpečnosti).

56. Zhotovitel je povinen poskytnout plnění dle Smlouvy řádně v souladu se Smlouvou a veškerými jejími přílohami, příslušnými ČSN, ČSN EN a českými i evropskými právními předpisy platnými a účinnými v době poskytování plnění.

57. Zhotovitel je povinen informovat Objednatele
    57.1. o kybernetických bezpečnostních incidentech souvisejících s plněním Smlouvy, a to ihned poté, co k incidentu dojde,
    57.2. o způsobu řízení rizik na straně Zhotovitele a o zbytkových rizicích souvisejících s plněním Smlouvy, a to do 5 pracovních dnů od nabytí účinnosti Smlouvy,
    57.3. o významné změně ovládání Zhotovitele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších přepisů (dále jen „**ZOK**"), nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Zhotovitelem k plnění podle Smlouvy, a to neprodleně poté, kdy k takové změně dojde.

58. Dojde-li k ukončení této Smlouvy jinak než splněním předmětu Smlouvy, je Zhotovitel povinen dle pokynů Objednatele učinit veškerá nezbytná bezpečnostní opatření ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) tak, aby ukončením této Smlouvy nedošlo k narušení bezpečnosti Významných informačních systémů, jejichž je Objednatel správcem.

59. Bude-li na základě této Smlouvy poskytována jakákoliv dokumentace v elektronické podobě, musí být předána v otevřeném, strojově čitelném formátu, např. *.pdf, nebo *.doc.

60. Získá-li Zhotovitel v souvislosti s plněním této Smlouvy jakákoliv data, která nebudou nezbytná pro splnění předmětu této Smlouvy, neprodleně taková data zlikviduje v souladu s pokyny

Objednatele a pravidly vyplývajícími z vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci (vyhláška o kybernetické bezpečnosti). Likvidaci ostatních získaných dat Zhotovitel provede stejným způsobem, a to neprodleně po splnění předmětu této Smlouvy. Zhotovitel je povinen si vždy před provedením likvidace dat vyžádat pokyny Objednatele.

IX. LICENCE, DATABÁZE

61. Zhotovitel tímto poskytuje Objednateli licenci nebo podlicenci, není-li oprávněn licenci poskytnout, na veškerý software, který má povahu autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, dodaný podle Smlouvy, ke kterému je oprávněn licenci nebo podlicenci poskytnout (dále jen „***Vlastní software***"), a to k okamžiku instalace či prvního užití Vlastního software v rámci plnění Smlouvy. Součástí licence k Vlastnímu software je oprávnění Objednatele dodaný Vlastní software jakkoliv měnit, spojit jej s jiným dílem nebo jej zařadit do díla souborného. V případě zániku Smlouvy jinak než splněním, nabývá Objednatel oprávnění dle tohoto odstavce k doposud dodanému Vlastnímu software okamžikem zániku Smlouvy.

62. Zhotovitel se zavazuje zajistit, aby nejpozději k okamžiku instalace softwaru dodaného podle Smlouvy, ke kterému Zhotovitel není oprávněn licenci nebo podlicenci poskytnout (dále jen „**Cizí software**"), byla Objednateli udělena licence na Cizí software (licence a podlicence k Vlastnímu a Cizímu software dále souhrnně též jen „***Licence na software***").

63. Licence na software se poskytuje, resp. musí být poskytnuta:
    63.1. jako bezúplatná;
    63.2. jako nevýhradní;
    63.3. z hlediska časového rozsahu na dobu trvání majetkových práv k předmětu Licence na software;
    63.4. z hlediska územního rozsahu na území České republiky;
    63.5. z hlediska věcného rozsahu (způsobu použití) tak, že opravňuje k takovým způsobům použití, aby Dílo bylo možné užívat k účelu vyplývajícímu ze Smlouvy;
    63.6. z hlediska osobního rozsahu (multilicence), resp. množství tak, že opravňuje k použití množství uživatelů či využití přístupů v množství dle Smlouvy, a není-li ve Smlouvě množství uvedeno, pak pro tolik uživatelů či přístupů, kolik jich je třeba k tomu, aby Dílo bylo možné užívat k účelu vyplývajícímu ze Smlouvy;
    nevyplývá-li ze Smlouvy jinak.

64. Zhotovitelem udělená Licence na Vlastní software se vztahuje ve shora uvedeném rozsahu i na jakákoli rozšíření, upgrady, updaty a patche Vlastního software.

65. Licenční smlouva obsahující Licenci na software bude součástí každé dodávky Cizího softwaru. Licence na Cizí software musí zahrnovat právo na jakákoli rozšíření, upgrady, updaty a patche po dobu trvání licence.

66. Objednatel není povinen Licenci na software využívat.

67. Součást Díla je též případná registrace Licencí na software na jméno Objednatele.

68. Vznikne-li během plnění Smlouvy nebo v souvislosti s plněním Smlouvy jakákoliv databáze, je pořizovatelem takové databáze Objednatel.

X. PŘEDÁNÍ A PŘEVZETÍ DÍLA

69. K předání Díla Zhotovitelem Objednateli a zároveň k převzetí Díla Objednatelem dochází dnem, v němž budou kumulativně splněny následující podmínky:
    69.1. budou úspěšně dokončeny penetrační testy,
    69.2. oběma Smluvními stranami bude podepsán předávací protokol o předání a převzetí Předávací dokumentace,
    69.3. Zhotovitel osadí pamětní desku.

70. Smluvní strany se dohodly, že § 1921, § 2112, § 2605 odstavec 2, § 2606, § 2609 a § 2618 Občanského zákoníku a rovněž obchodní zvyklosti, jež jsou svým smyslem nebo účinky stejné nebo obdobné uvedeným ustanovením, se nepoužijí.

XI. NABYTÍ VLASTNICKÉHO PRÁVA A PŘECHOD NEBEZPEČÍ ŠKODY

71. Vlastnické právo ke zhotovovanému Dílu má bez jakýchkoli výjimek od počátku Objednatel, přičemž vlastnické právo k jakékoliv věci, která je součástí plnění poskytovaného Zhotovitelem dle Smlouvy, přechází na Objednatele jejím zabudováním do sítě či informačního systému Objednatele, po její instalaci v nich, nebo jejím prostým dodáním (jde-li o samostatnou věc, která je součástí Díla) do místa plnění. Objednatel zůstává vlastníkem Díla i v případě zániku závazků ze Smlouvy jinak než splněním.

72. Nebezpečí škody na Díle a věcech, které předal Zhotovitel Objednateli za účelem splnění svých povinností, přechází na Objednatele okamžikem převzetí Díla Objednatelem.

73. Smluvní strany se dohodly, že § 1976, § 2599 – 2603 a § 2624 Občanského zákoníku a rovněž obchodní zvyklosti, jež jsou svým smyslem nebo účinky stejné nebo obdobné uvedeným ustanovením, se nepoužijí.

XII. VADY DÍLA A ZÁRUČNÍ PODMÍNKY

74. Zhotovitel poskytuje Objednateli záruku za jakost poskytnutého plnění, jíž se zavazuje, že poskytnuté plnění bude po záruční dobu způsobilé pro použití k účelu vyplývajícímu z odstavce 13 Smlouvy, zachová si obvyklé vlastnosti, bude prosté jakýchkoliv vad a nebude mít právní vady. Dílo má právní vadu, pokud k němu uplatňuje právo třetí osoba.

75. Dílo bude vadné, zejm. nebude-li:
    75.1. při převzetí Objednatelem mít vlastnosti sjednané Smlouvou nebo
    75.2. kdykoli v průběhu Záruční doby způsobilé pro použití k účelu vyplývajícímu ze Smlouvy nebo
    75.3. kdykoli v průběhu Záruční doby mít vlastnosti sjednané Smlouvou nebo
    75.4. při převzetí Objednatelem nebo kdykoli v průběhu Záruční doby prosté právních vad.

76. Záruční doba činí 36 měsíců (dále jen „**Záruční doba**"). Záruční doba začíná běžet dnem převzetí Díla Objednatelem.

77. Objednatel má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Smlouvy nebo při převzetí Díla.

78. Zhotovitel nenese odpovědnost za vady způsobené Objednatelem nebo jinými osobami, ledaže Objednatel nebo takové osoby postupovaly v souladu s dokumenty nebo pokyny, které obdržely od Zhotovitele.

79. Objednatel nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na Díle na Objednatele vnější událost. To neplatí, způsobil-li vadu Zhotovitel nebo jakákoliv jiná osoba, jejímž prostřednictvím plnil své povinnosti vyplývající ze Smlouvy.

80. Odpovídá-li Zhotovitel za vady Díla, má Objednatel práva z vadného plnění.

81. Odstraňování vad Díla bude probíhat za podmínek stanovených v servisní smlouvě č. [redacted] uzavřené mezi Objednatelem a Zhotovitelem jako poskytovatelem servisních služeb na základě výsledků Řízení veřejné zakázky (dále jen *„servisní smlouva"*).

82. Vznikne-li nebo projeví-li se na Díle během Záruční doby vada, za kterou Zhotovitel odpovídá, je Zhotovitel povinen vadu odstranit za podmínek a ve lhůtách stanovených v servisní smlouvě. Není-li pro konkrétní vadu v servisní smlouvě stanovena doba pro její odstranění, je Zhotovitel povinen takovou vadu odstranit bez zbytečného odkladu od oznámení vady Objednatelem.

83. Nebude-li vada odstraněna v době dle předchozího odstavce, má Objednatel právo zajistit odstranění vady jinou odborně způsobilou osobou na náklady Zhotovitele nebo na přiměřenou slevu z Ceny Díla nebo od Smlouvy odstoupit; to neplatí u vady, která se ukáže jako neodstranitelná, v takovém případě má Objednatel právo na přiměřenou slevu z Ceny Díla nebo od Smlouvy odstoupit.

84. Veškeré náklady vzniklé Objednateli v souvislosti s odstraněním vady způsobem podle předchozího odstavce Smlouvy je Zhotovitel povinen Objednateli uhradit. Zhotovitel se tak zejména zavazuje uhradit cenu účtovanou Objednateli jinou odborně způsobilou osobou.

85. Smluvní strany se dohodly, že § 1917 - 1924, § 2099 – 2101, § 2103 - 2117 a § 2165 - 2172 Občanského zákoníku a rovněž obchodní zvyklosti, jež jsou svým smyslem nebo účinky stejné nebo obdobné uvedeným ustanovením, se nepoužijí.

XIII. BANKOVNÍ ZÁRUKA

86. Zhotovitel je povinen sjednat ve prospěch Objednatele bankovní záruku za řádné provedení Díla ve výši **500 000,-** Kč (dále jen *„**Bankovní záruka za provedení**"*). Bankovní záruka za provedení bude krýt jakékoli pohledávky Objednatele za Zhotovitelem vzniklé Objednateli z důvodu porušení jedné či více povinností Zhotovitele týkajících se provedení Díla ve smluvené kvalitě a době, včetně případné škody a nemajetkové újmy způsobené Zhotovitelem porušením Smlouvy nebo v souvislosti s prováděním Díla, do okamžiku převzetí Díla Objednatelem.

87. Zhotovitel je povinen předat Objednateli originál záruční listiny Bankovní záruky za provedení vystavené bankou nejpozději do 15 pracovních dnů po nabytí účinnosti Smlouvy.

88. Bankovní záruka za provedení musí být platná a účinná ode dne jejího předání Objednateli nejméně do konce kalendářního měsíce, který následuje po kalendářním měsíci, ve kterém Objednatel převzal Dílo. Vzhledem ke skutečnosti, že konec doby podle předchozí věty nelze předem stanovit konkrétním datem, zavazuje se Zhotovitel předložit Objednateli záruční listinu na bankovní záruku, jež bude platná a účinná nejméně do 31. 12. 2019.

89. Nepřevezme-li Objednatel Dílo nejpozději 1 měsíc před skončením platnosti Bankovní záruky za provedení, je Zhotovitel povinen prodloužit platnost Bankovní záruky za provedení nejméně o další 3 měsíce a nejpozději 15 dní před skončením dosavadní platnosti Bankovní záruky za provedení předat prodlouženou Bankovní záruku za provedení Objednateli.

90. Zhotovitel je povinen sjednat ve prospěch Objednatele bankovní záruku za jakost Díla ve výši **500 000,-** Kč (dále jen ***„Bankovní záruka za jakost"***). Bankovní záruka za jakost bude krýt jakékoli pohledávky Objednatele za Zhotovitelem vzniklé Objednateli z důvodu porušení jedné či více povinností Zhotovitele vyplývajících z odpovědnosti Zhotovitele:
    90.1. za vady Díla;
    90.2. za prodlení s odstraněním vad Díla,
    90.3. za náklady na odstranění vady vynaložené Objednatelem.

91. Zhotovitel je povinen předat Objednateli originál záruční listiny Bankovní záruky za jakost vystavené bankou nejpozději při převzetí Díla Objednatelem.

92. Bankovní záruka za jakost musí být platná a účinná ode dne jejího předání Objednateli nejméně do uplynutí 1 měsíce od ukončení trvání Záruční doby.

93. Bankovní záruka za provedení a Bankovní záruka za jakost budou dále označovány společně jen jako ***„Bankovní záruka"***.

94. Bankovní záruka musí být neodvolatelná, nepodmíněná a splatná na první výzvu bez jakýchkoliv námitek.

95. Objednatel musí být v záruční listině Bankovní záruky označen jako osoba oprávněná čerpat Bankovní záruku.

96. Zhotovitel je povinen do 15 pracovních dnů po každém čerpání Bankovní záruky Objednatelem předat Objednateli novou Bankovní záruku ve shodném znění a výši jako měla čerpaná Bankovní záruka, případně Bankovní záruku doplnit do původní sjednané výše.

97. Objednatel je po skončení platnosti Bankovní záruky povinen vrátit záruční listinu zpět Zhotoviteli do jednoho měsíce od doručení výzvy Zhotovitele k vrácení Bankovní záruky.

XIV. SANKCE

98. V případě prodlení Zhotovitele s provedením Díla je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,2 % z Ceny Díla za každý i započatý den prodlení.

99. V případě prodlení Zhotovitele s úspěšným dokončením kterékoliv části kterékoliv etapy Díla je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,2 % z ceny příslušné etapy Díla, s níž, nebo s jejíž částí je Zhotovitel v prodlení, za každý i započatý den prodlení.

100. Poruší-li Zhotovitel povinnost předat Objednateli originál záruční listiny k Bankovní záruce v době dle odstavce 87 nebo odstavce 91 Smlouvy, nebo poruší-li Zhotovitel povinnost předat Objednateli Bankovní záruku za plnění prodlouženou ve smyslu odstavce 89 Smlouvy v době dle uvedeného odstavce, je povinen uhradit Objednateli smluvní pokutu ve výši 0,5% z částky dle odstavce 86 nebo odstavce 90 Smlouvy za každý i započatý den prodlení.

101. Poruší-li Zhotovitel jakoukoliv povinnost podle odstavce 118, 119 nebo 131 až 135 Smlouvy, je povinen uhradit Objednateli smluvní pokutu ve výši 0,1 % z Ceny Díla za každé jednotlivé porušení.

102. Zaplacení smluvní pokuty nezbavuje Zhotovitele povinnosti splnit dluh smluvní pokutou utvrzený.

103. Objednatel je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinnosti Zhotovitele, na kterou se vztahuje smluvní pokuta, v plné výši.

XV. ODSTOUPENÍ OD SMLOUVY

104. Objednatel je oprávněn od Smlouvy odstoupit z důvodů stanovených právními předpisy nebo sjednaných Smlouvou. Objednatel je oprávněn odstoupit od Smlouvy ohledně celého plnění i v případě, že Zhotovitel již zčásti plnil.

105. Objednatel je oprávněn odstoupit od Smlouvy zejména:
    105.1. bude-li Zhotovitel v prodlení s úspěšným dokončením kterékoliv části kterékoliv etapy Díla o více než 30 dnů;
    105.2. bude-li Zhotovitel v prodlení s provedením Díla o více než 30 dnů;
    105.3. ukáže-li se jako nepravdivé jakékoliv prohlášení Zhotovitele uvedené ve Smlouvě;
    105.4. ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku;
    105.5. jestliže Zhotovitel bezdůvodně přeruší provádění Díla;
    105.6. jestliže Zhotovitel neodstraní v průběhu provádění Díla vady zjištěné Objednatelem v dodatečné lhůtě stanovené písemně Objednatelem;
    105.7. jestliže Zhotovitel poruší některou svoji povinnost uvedenou v odstavci 118, 119 nebo 131 až 135 Smlouvy;
    105.8. poruší-li Zhotovitel jakoukoliv povinnost dle Smlouvy podstatným způsobem;
    105.9. bude-li Zhotovitel pravomocně odsouzen za trestný čin;
    105.10. bude-li Zhotoviteli uložen zákaz plnění veřejných zakázek;
    105.11. v případě významné změny ovládání Zhotovitele dle ZOK nebo významné změny kontroly nad Zhotovitelem, nebo změny vlastnictví zásadních aktiv, využívaných Zhotovitelem k plnění podle Smlouvy, popřípadě změny oprávnění nakládat s těmito aktivy nebo změny kontroly nad nimi.

XVI. POSTUP PŘI ZÁNIKU SMLOUVY JINAK NEŽ SPLNĚNÍM

106. V případě zániku Smlouvy jinak než splněním provedou Objednatel a Zhotovitel kontrolu rozsahu, stavu a kvality doposud poskytnutého plnění a zjištěný stav uvedou ve zjišťovacím protokolu. Zhotovitel zpracuje veškerou Předávací dokumentaci k Dílu v jeho stávající podobě a rozsahu a předá ji Objednateli.

107. Ustanovení Smlouvy o odpovědnosti za vady a poskytnutí Záruční doby se na Zhotovitelem poskytnuté plnění použijí obdobně, Záruční doba na plnění poskytnuté do zániku Smlouvy počíná běžet zánikem Smlouvy.

108. Ujednání Smluvních stran ve Smlouvě o odpovědnosti za vady Díla, o odpovědnosti za škodu a nemajetkovou újmu, o sankcích, ujednání dle odstavce 106 a ujednání Smlouvy, která dle své povahy mají trvat a Smluvní strany zavazovat i po zániku Smlouvy, budou trvat a Smluvní strany zavazovat i po zániku Smlouvy.

XVII. PROHLÁŠENÍ SMLUVNÍCH STRAN

109. Zhotovitel prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Zhotovitel dále prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Zhotovitele a že mu není známo, že by vůči němu takové řízení bylo zahájeno.

110. Zhotovitel na sebe přebírá nebezpečí změny okolností ve smyslu § 1765 Občanského zákoníku.

111. Vzhledem k veřejnoprávnímu charakteru Objednatele Zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Smlouvy v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

112. Zhotovitel si je vědom, že je ve smyslu § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly.

113. Zhotovitel je povinen řádně uchovávat veškerou dokumentaci a účetní doklady související s realizací Díla minimálně do konce roku 2030. Pokud je v českých právních předpisech stanovena lhůta delší než v evropských předpisech, musí být použita pro úschovu delší lhůta.

114. Zhotovitel je povinen minimálně do konce roku 2030 poskytovat požadované informace a dokumentaci vztahující se k Dílu zaměstnancům nebo zmocněncům pověřených orgánů (Centra pro regionální rozvoj ČR, Ministerstva pro místní rozvoj ČR (dále jen „**MMR**"), Ministerstva financí ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, Auditního orgánu (dále jen „**AO**"), Platebního a certifikačního orgánu (dále jen „**PCO**"), příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen informovat Objednatele o skutečnostech majících vliv na realizaci Díla, především pak povinnost informovat o jakýchkoli kontrolách a auditech provedených v souvislosti s Dílem; dále též povinnost na žádost MMR, Řídícího orgánu Operačního programu, PCO nebo AO poskytnout veškeré informace o výsledcích a kontrolní protokoly z těchto kontrol a auditů. A zároveň vytvořit podmínky k provedení kontroly a poskytnout při provádění kontroly součinnost.

115. Smluvní strany prohlašují, že identifikační údaje uvedené v článku I Smlouvy odpovídají aktuálnímu stavu a že osobami jednajícími při uzavření Smlouvy jsou osoby oprávněné k jednání za Smluvní strany bez jakéhokoliv omezení vnitřními předpisy Smluvních stran.

116. Jakékoliv změny údajů uvedených v článku I Smlouvy, jež nastanou v době po uzavření Smlouvy, jsou Smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé Smluvní straně.

117. V případě, že se kterékoliv prohlášení některé ze Smluvních stran uvedené ve Smlouvě ukáže býti nepravdivým, odpovídá tato Smluvní strana za škodu a nemajetkovou újmu, které nepravdivostí prohlášení nebo v souvislosti s ní druhé Smluvní straně vznikly.

XVIII. POJIŠTĚNÍ

118. Zhotovitel se zavazuje, že bude mít po celou dobu trvání závazku vyplývajícího ze Smlouvy až do doby uplynutí Záruční doby sjednáno pojištění odpovědnosti za škodu či jinou újmu způsobenou Zhotovitelem při výkonu činnosti jiné osobě s limitem pojistného plnění minimálně ve výši Ceny Díla. V případě, že Smlouvu uzavřelo na straně Zhotovitele více osob (členů sdružení, členů

společnosti apod.), musí pojistná smlouva prokazatelně pokrývat případnou škodu či jinou újmu způsobenou kteroukoli z těchto osob.

119. Zhotovitel je povinen předložit Objednateli pojistnou smlouvu nebo pojistku osvědčující splnění povinnosti Zhotovitele podle předchozího odstavce Smlouvy do 15 dnů ode dne nabytí účinnosti Smlouvy a dále kdykoli v průběhu trvání závazků ze Smlouvy bezodkladně poté, kdy k tomu byl Objednatelem vyzván.

120. Zhotovitel i Objednatel se zavazují uplatnit pojistnou událost u pojišťovny bez zbytečného odkladu.

XIX. OSTATNÍ UJEDNÁNÍ

121. Tvoří-li Zhotovitele více osob, platí následující:
    121.1. všechny osoby tvořící Zhotovitele jsou ze Smlouvy zavázány společně a nerozdílně,
    121.2. jednání kterékoli z osob tvořících Zhotovitele je přičítáno Zhotoviteli bez ohledu na vnitřní vztahy mezi jednotlivými osobami tvořícími Zhotovitele,
    121.3. za Zhotovitele může jednat kterákoli z osob tvořících Zhotovitele.

122. Zhotovitel je povinen neprodleně písemně informovat Objednatele o skutečnostech majících i potenciálně vliv na plnění jeho povinností vyplývajících ze Smlouvy, a není-li to možné, nejpozději následující den poté, kdy příslušná skutečnost nastane nebo Zhotovitel zjistí, že by nastat mohla. Současně je Zhotovitel povinen učinit veškeré nezbytné kroky vedoucí k eliminaci případné škody hrozící Objednateli, a to zejména obstarat neprodleně náhradní plnění, přičemž je povinen nést případný rozdíl ceny.

123. Zhotovitel bere na vědomí, že Objednatel je povinným subjektem podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

124. Zhotovitel souhlasí se zveřejněním Smlouvy v souladu s povinnostmi Objednatele za podmínek vyplývajících z příslušných právních předpisů, zejména souhlasí se zveřejněním Smlouvy, včetně všech jejích změn a dodatků, výše skutečně uhrazené ceny na základě Smlouvy a dalších údajů na profilu zadavatele Objednatele podle Zákona o zadávání veřejných zakázek a v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „***Zákon o registru smluv***"). Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 Zákona o registru smluv splní Objednatel. Zhotovitel prohlašuje, že Smlouva ani žádná její část nejsou obchodním tajemstvím Zhotovitele ve smyslu § 504 Občanského zákoníku.

125. Zhotovitel je povinen chránit osobní údaje a při jejich ochraně postupovat v souladu s příslušnými právními předpisy, zejména zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Zhotovitel je povinen dodržovat podle Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27.04.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), povinnost zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.

126. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy nebo vzniklou v souvislosti se Smlouvou.

127. Zhotovitel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou na jakoukoliv pohledávku Objednatele za Zhotovitelem.

128. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Zhotovitelem vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou (zejména smluvní pokutu) na jakoukoliv splatnou i nesplatnou pohledávku Zhotovitele za Objednatelem.

129. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsažené ve Smlouvě a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl v souvislosti se Smlouvou, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou. Zhotovitel nesmí takové skutečnosti a informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo jiných osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti podle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku závazku ze Smlouvy, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti podle tohoto odstavce se nevztahují na případy, kdy je Zhotovitel povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.

130. Poruší-li Zhotovitel v souvislosti se Smlouvu jakoukoli svoji povinnost, nahradí Objednateli škodu a nemajetkovou újmu z toho vzniklou. Povinnosti k náhradě se Zhotovitel zprostí, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezprostí.

XX. PODDODAVATELÉ

131. Zhotovitel je oprávněn pověřit plněním svých povinností vyplývajících ze Smlouvy pouze jiné osoby uvedené v příloze č. 10 Smlouvy, nebo osoby písemně odsouhlasené Objednatelem (dále jen jednotlivě „***Poddodavatel***" nebo společně „***Poddodavatelé***").

132. Zhotovitel odpovídá za plnění Poddodavatele tak, jako by plnil sám. Objednatel je povinen vybírat Poddodavatele tak, aby Poddodavatelé nebyli v rozporu s požadavky Objednatele na Zhotovitele.

133. Zhotovitel prohlašuje a zavazuje se, že jako ručitel uspokojí za jakéhokoliv Poddodavatele jeho povinnost nahradit újmu způsobenou Poddodavatelem Objednateli při plnění nebo v souvislosti s plněním povinností ze Smlouvy, jestliže Poddodavatel povinnost k náhradě újmy nesplní. Objednatel Zhotovitele jako ručitele podle předchozí věty přijímá.

134. Objednatel je oprávněn požadovat a Zhotovitel je povinen zabezpečit změnu Poddodavatele nebo část Díla prováděnou Poddodavatelem provést sám, splňuje-li všechny pro plnění příslušné části Díla Objednatelem stanovené předpoklady a kvalifikaci, a to v případech, kdy:
    134.1. bude Poddodavatel vůči Objednateli v prodlení se splněním povinnosti z jiného závazku nebo
    134.2. bude Poddodavatel pravomocně odsouzen za trestný čin nebo
    134.3. se Poddodavatel ocitne ve stavu úpadku nebo hrozícího úpadku nebo
    134.4. bude Poddodavateli uložen zákaz plnění veřejných zakázek nebo

134.5. bude dán jiný závažný důvod pro změnu Poddodavatele (např. důvod obdobný důvodu pro odstoupení Objednatele od Smlouvy).

Zhotovitel je povinen navrhnout nového Poddodavatele do 10 dnů od doručení žádosti Objednatele. Nový Poddodavatel může být připuštěn k plnění Díla výlučně na základě písemného souhlasu Objednatele.

135. Zhotovitel je oprávněn změnit Poddodavatele z důvodů na straně Zhotovitele pouze s předchozím písemným souhlasem Objednatele.

XXI. ZÁVĚREČNÁ UJEDNÁNÍ

136. Přílohy Smlouvy jsou její nedílnou součástí.

137. Veškerá práva a povinnosti Smluvních stran vyplývající ze Smlouvy se řídí českým právním řádem. Smluvní strany se dohodly, že ustanovení právních předpisů, která nemají donucující účinky, mají přednost před obchodními zvyklostmi, pokud Smlouva nestanoví jinak.

138. Všechny spory vznikající ze Smlouvy a v souvislosti s ní budou podle vůle Smluvních stran rozhodovány soudy České republiky, jakožto soudy výlučně příslušnými.

139. Smlouvu lze měnit pouze písemnými dodatky. Jakékoli změny Smlouvy učiněné jinou než písemnou formou jsou vyloučeny.

140. Smlouva je sepsána ve čtyřech vyhotoveních, z nichž Objednatel obdrží 3 vyhotovení a Zhotovitel 1 vyhotovení.

141. Smlouva nabývá platnosti dnem jejího uzavření.

142. Smlouva nabývá účinnosti uveřejněním v registru smluv dle Zákona o registru smluv.

143. Uzavření této smlouvy bylo schváleno usnesením Rady Olomouckého kraje č. UR/65/51/2019 ze dne 20. 5. 2019.

Přílohy

Příloha č. 1	První etapa
Příloha č. 2	Druhá etapa
Příloha č. 3	Třetí etapa
Příloha č. 4	Čtvrtá etapa
Příloha č. 5	Pátá etapa
Příloha č. 6	Penetrační testy
Příloha č. 7	Podrobná technická specifikace nabízeného hardwaru a softwaru
Příloha č. 8	Položkový rozpočet
Příloha č. 9	Harmonogram
Příloha č. 10	Poddodavatelé

V OLOMOUCI dne 05-06-2019

[redacted]

Olomou
Ladislav Okle[redacted]

V OLOMOUCI dne 3.6.2019

[redacted]

MERIT GROUP a.s.
Petr Weigel, statutární ředitel

Příloha č. 1 Smlouvy

První etapa - Web aplikační firewall

Technická a implementační specifikace

High-level popis požadovaného řešení

Webové aplikace publikované do vnějších sítí, zejména veřejné sítě Internet, mohou být náchylné na zranitelnosti vůči kybernetickým útokům a aplikačním DoS a DDoS útokům. Nasazením webového aplikačního firewallu (WAF) je možné provádět inspekci webové komunikace a ochranu před kybernetickými útoky. Zároveň je nutné zajistit vysokou dostupnost, rozklad zátěže - loadbalancing a funkci Reverzního proxy serveru aplikací prostřednictvím komponenty Application Delivery Controller (ADC).
Požadujeme dvojici HW zařízení v roli WAF a ADC. Dvojice HW řešení WAF a ADC bude publikovat definované služby, oddělovat reálné servery od přistupujících uživatelů, modifikovat a provádět inspekci webového provozu. Pokud zařízení neumožňuje integrovat obě funkcionality, může být dodáno jako separátní dvojice WAF zařízení a separátní dvojice ADC.
Řešení bude koncipované jako redundantní a vysoce dostupný cluster a bude fungovat v režimu Active-Active nebo Active-Standby. Řešení bude odpovědné za monitoring dostupných aplikací služeb, řízení distribuce a zátěže aplikačního provozu mezi servery, které budou jednotlivé aplikace a služby poskytovat. Řešení bude také zodpovědné za optimalizaci a modifikaci aplikačního provozu s cílem efektivně využívat zdroje aplikace nebo zamezit nežádoucí distribuci dat k uživatelům (např. manipulace s HTTP záhlavím, HTML kódem apod. šifrování cookies apod.). Řešení bude také zodpovědné za optimalizaci TCP provozu, HTTP kompresi a související optimalizaci aplikačního provozu.
Implementaci politik a pravidel pro řízení aplikačního předpokládáme minimálně v rozsahu:

- Zapojení a integrace v prostředí Zákazníka
- Vytvoření HA clusteru
- Monitoring zdraví aplikací a služeb
- SSL terminace, management SSL certifikátů
- Napojení na monitorovací a logovací nástroje
- Reverzní proxy s funkcí NAT44, případně NAT 46, NAT 64
- Optimalizace HTTP provozu (HTTP komprese)
- Zabezpečení HTTP provozu (cookies, manipulace s HTTP záhlavím apod.)

Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu. K těmto základním bezpečnostním politikám předpokládáme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem. Dále požadujeme, aby WAF obsahoval technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní vyhledávače Googlebot, Seznambot apod.). WAF také zajistí ochranu před únosy HTTP relací. WAF musí podporovat SSL terminaci, jelikož HTTP protokol bude šifrován.
Řešení musí být realizováno ve vysoké dostupnosti v režimu minimálně "active-standby".
Implementace bezpečnostních politik bude minimálně v rozsahu:

- Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.)
- Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10

- Ochrana proti manipulaci s cookies
- Ochrana parametrů webové aplikace
- Session Management – ochrana proti únosům relací
- Brute Force Ochrana – ochrana před prolomení hrubou silou
- Detekce robotických uživatelů aplikace u vybraných aplikací

Ostatní požadavky na funkcionality webového aplikačního firewallu jsou uvedeny v tabulce technické specifikace. V případě integrace funkce WAF s funkcí ADC v jednom HW zařízení je přípustné, aby požadavky na propustnost L4, L7, SSL a fyzické připojení byly splněny v pouze tomto jednom zařízení.

Technická specifikace zařízení a SW

Technická specifikace řešení WAF

Pol. č.	*Technické požadavky na WAF*
1	2 ks samostatného HW zařízení s montáží do technologické 19" skříně (RACK), max. 2U nebo jako rozšiřující licence k ADC
2	V případě samostatného HW zařízení WAF plně redundantní napájecí zdroj AC
3	V případě samostatného HW zařízení WAF požadujeme min. 6x 1Gbps optických Ethernet rozhraní nebo slotů a zároveň min. 4 x 10 Gbps optických rozhraní nebo slotů pro Ethernet
4	V případě samostatného HW zařízení WAF, které obsahuje sloty pro optická rozhraní, požadujeme celkem 4x Ethernet moduly s podporou rychlosti 10 Gbps s vlnovou délkou 850 nm pro vlákno MMF (50/125)
5	V případě samostatného HW zařízení WAF Lights-out management - nezávislý servisní procesor pro vzdálenou správu zařízení (vypnutí/zapnutí zařízení, konzolový přístup)
6	L4 propustnost každého HW zařízení minimálně 18 Gbps
7	L7 propustnost každého HW zařízení minimálně 18 Gbps
8	Každé HW zařízení podporuje minimálně 425 000 L4 spojení za sekundu
9	Každé HW zařízení podporuje minimálně 20 milionů současných TCP/UDP spojení
10	Každé HW zařízení podporuje minimálně 18000 SSL transakcí za vteřinu pro RSA klíče s délkou 2048-bitů
11	Každé HW zařízení podporuje minimálně 9000 SSL transakcí za vteřinu pro klíče ECDSA s P-256
12	Vestavěná ochrana proti HTTP DoS útokům
13	Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10
14	Možnost doprogramovat si filtrovací pravidla pro aplikace
15	Ochrana AJAX a JSON aplikací
16	Detekce a ochrana před web scraping útoky
17	Detekce a ochrana před pokusy o prolomení logovacích stránek pomocí hrubé síly (brute force)
18	Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům)
19	Rozšířená podpora pro detekci aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu, detekce robotických klientů
20	Podpora odlišení lidských uživatelů od robotů pomocí Captcha
21	Zabezpečení XML komunikace
22	Podpora maskování/odstranění citlivých informací – např. rodné čísla, čísla kreditních karet apod.
23	Automatické nahrávání a aplikování nových signatur aplikačních útoků
24	Podpora pro vytváření vlastních signatur pro detekci HTTP útoků
25	Podpora pozitivního a negativního bezpečnostního modelu (pozitivní a negativní bezpečnostní logika)
26	Blokování útočníků na základě geolokace
27	Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP

28	Ochrana protokolů SMTP a FTP
29	Podpora SSL (šifrování a dešifrování)
30	Podpora ECDSA a podpora hybridních certifikátů (DSA/ECDSA/RSA)
31	Popdora symetrického šifrování včetně šifer Camellia
32	Podpora HTTP Strict Transport Security (HSTS)
33	Podpora HTTP/2
34	Podpora akcelerace
	- Konsolidace TCP spojení od klienta směrem k serveru tj. Z několika spojení od uživatele udělat jedno spojení na server
	- Caching
	- Komprese
	- Možnost optimalizace TCP stacku zvlášť směrem k uživateli a směrem k severu
35	Podpora různých typů reportů – PCI, geolokační reporty
36	Podpora standardů PCI DSS, HIPAA, Basel II a SOX
37	Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint aj.
38	Integrace s nástrojem na detekci zranitelností webových aplikací
39	Podpora pro monitoring a měření výkonu HTTP aplikací
40	Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů:
	· Cenzic Hailstorm
	· WhiteHat Sentinel
	· IBM Rational AppScan
	· QualysGuard Web Application Scanning
41	Podpora REST API pro správu zařízení
42	Autentikace klientů přes LDAP/Radius
43	Certifikace ICSA webového aplikačního firewallu
44	Možnost připojení k monitorovacím nástrojů třetích stran prostřednictvím otevřeného API
45	Možnost přidávat zákaznické požadavky na základě skriptovacího jazyka nebo obdobné technologie
46	Podpora Active-Active, Active-Passive módů
47	Granulární logování / logování per aplikace
48	K dispozici jako autonomní box nebo ve formě šasi
49	Management: sériový port, GUI, příkazový řádek, iLO
50	Podpora login a logout stránek pomocí AJAX/JSON
51	Mitigace DDoS útoků založená na behaviorální analýze
52	Povoleni jednotlivych HTTP metod pro jednotliva URL
53	Podpora více logovacích profilů pro danou aplikaci
54	Podpora WebSocketu
55	Prevence před únosy klientských HTTP relací „Session Hijacking"
56	Detekce anomalií sledovanim ID koncove stanice uzivatele
57	Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům)
58	Podpora virtualizace – separací IP adresního prostoru (obdoba VRF) nebo plnohodnotné virtualizace
59	Možnost rozšíření o funkci Web Aplikačního Firewalu dodatečnou licencí
60	Možnost rozšíření o funkci podpory externích šifrovacích karet (HSM) dodatečnou licencí

Technická specifikace funkcí ADC

Pol. č.	*Technické požadavky na proxy server (ADC)*
1	2 ks HW zařízení s montáží do technologické 19" skříně (RACK), max. 2U
2	Plně redundantní napájecí zdroje AC
3	Požadujeme min. 6x 1Gbps optických Ethernet rozhraní nebo slotů a zároveň min. 4 x 10 Gbps optických rozhraní nebo slotů pro Ethernet
4	Požadujeme celkem 4x Ethernet moduly s podporou rychlosti 10 Gbps s vlnovou délkou 850 nm pro vlákno MMF (50/125)
5	Lights-out management - nezávislý servisní procesor pro vzálenou správu zařízení (vypnutí/zapnutí zařízení, konzolový přístup)
6	L4 propustnost každého HW zařízení minimálně 18 Gbps
7	L7 propustnost každého HW zařízení minimálně 18 Gbps
8	Každé HW zařízení podporuje minimálně 425 000 L4 spojení za sekundu
9	Každé HW zařízení podporje minimálně 20 milionů současných TCP/UDP spojení
10	Každé HW zařízení podporuje minimálně 18000 SSL transakcí za vteřinu pro RSA klíče s délkou 2048-bitů
11	Každé HW zařízení podporuje minimálně 9000 SSL transakcí za vteřinu pro klíče ECDSA s P-256
12	Podpora SSL certifikátů podepsaných SHA-2 metodou
13	Podpora TLS 1.2
15	Podpora AES-GCM a ECC pro TLS 1.2
16	Podpora STARTTLS pro SMTP provoz
17	Podpora šifrování pomocí Suite B, ECDSA, AES-GCM
18	Popdora symetrického šifrování včetně šifer Camellia
19	Podpora HTTP Strict Transport Security (HSTS)
20	Možnost pracovat až s 4096-bitovými klíči
21	Podpora hardwarové SSL akcelerace
22	Možnost zvýšit výkonnostní parametry SSL dokoupením licence
	Balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů až do 7. vrstvy OSI (ftp, dns, https/http, sip, ...)
	Klient/Server NAT/PAT
	Podpora různých typů rozkladu zátěže provozu:
	· Kruhová metoda s vážením
	· Podle počtu navázaných spojení
	· Podle otisku zdrojové a cílové adresy
	· Podle URL a cookie
23	· Na základě SNMP (např. zátěže procesorů)
24	· Podle vah pro skupiny
25	· Na základě počtu odezev od serverů
26	Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, L4 payloadu, HTTP cookie, HTTP obsahu, HTTP hlavičky, RADIUS atributů, RTSP hlavičky, SIP hlavičky, SSL Session ID
27	Podpora různých typů dostupnosti a zdraví aplikace (monitoring) - ICMP, DNS, HTTP, TCP/UDP port, SSL Hello, SMTP, RADIUS, LDAP, WMI...

28	Možnost kombinace více metod monitoringu (AND/OR)
29	Podpora modifikace HTTP provozu:
	· Vložení/přepsání cookie
	· Modifikace URL
	· Možnost vložit zdrojovou IP do L7 hlavičky
	· Modifikace HTTP obsahu
30	Podpora šablon pro konfiguraci balancingu aplikací – např. Microsoft Exchange Server 2010 a 2013 Client Access Servers,Citrix XenApp a XenDesktop
31	Možnost tyto šablony upravovat dle potřeb zákazníka
32	Podpora TCP multiplexingu
33	Podpora multipath TCP (MPTCP)
34	Podpora symetrické akcelerace Citrix ICA
35	Podpora ICAP protokolu
36	Podpora http komprese
37	Podpora http mezipaměti (cache)
38	Podpora filtrování paketů
39	Podpora QoS – markování, rate-limiting
40	Podpora TCP SYN cookie ochrany
41	Podpora SDN služeb – VXLAN virtualizace sítě
42	Podpora NVGRE a Transparent Ethernet Bridging tunelu
43	TDS/ MSSQL DB Proxy
44	Podpora Financial Information eXchange (FIX) protokolu
45	Podpora pro monitoring, manipulaci a modifikaci dat procházejícího datového provozu na základě skriptovacího jazyka nebo obdobné technologie
46	Podpora protokolu HTTP/2
47	Podpora IPv4/IPv6 brány
48	Plná podpora IPv6
49	Podpora 802.1Q
50	Podpora sFlow
51	Podpora IPFIX
52	Správa přes GUI, CLI
53	Podpora SNMP (1, 2c a 3)
54	Podpora SSH
55	Podpora vysokorychlostního logování pro každou aplikaci zvlášť
56	Podpora režimu redundance se synchronizací stavových tabulek (state failover)
57	Podpora redundantních clusterů Active-Standby i Active-Active
58	Možnost zapojit do redundantniho clusteru různé typy HW nebo virtualizovaných platforem
59	Dostupnost jak hardwarového tak i virtuálního řešení
60	Podpora otevřeného API pro nástroje třetích stran pro konfiguraci a monitoring zařízení
61	Podpora virtualizace – separací IP adresního prostoru (obdoba VRF) nebo plnohodnotné virtualizace
62	Možnost rozšíření o funkci Web Aplikačního Firewalu dodatečnou licencí
63	Možnost rozšíření o funkci podpory externích šifrovacích karet (HSM) dodatečnou licencí

Specifikace implementačního procesu

První část - Specifikace implementačního procesu a požadovaných produktů a výstupů řešení WAF

- Dodavatel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie webového aplikačního firewallu, jejíž obsah bude následující:
    - Popis terminologie, použité v dokumentu
    - Informace o stávajícím prostředí Zákazníka
    - Seznam aplikací, které budou WAF zabezpečeny
    - High-level popis řešení
    - Popis změny v infrastruktuře
    - High-level popis úpravy ovlivněných procesů např. řešení bezpečnostních incidentů
    - Řešení autentizace administrátorů WAF protokolem TACACS+
- Dodavatel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
    - Vymezení rozsahu řešení
    - Popis funkčních vlastností požadovaného zabezpečení aplikací technologií WAF
    - Popis úprav existujícího IT prostředí Zákazníka
    - Popis cílové úpravy vnitřních procesů
- Dodavatel vytvoří Low Level Design s následujícím obsahem:
    - Celkový návrh řešení
    - Typizované konfigurační šablony bezpečnostních politik WAF
    - Konfigurace WAF clusteru (zajištění konzistence bezpečnostních politik napříč clusterem WAF)
    - Konfigurace bezpečnostních politik
    - Ladění bezpečnostních politiky proti výskytu tzv. falešných poplachů
    - Konfigurace ochrany proti DoS a DDoS aplikačním útokům
    - Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace
    - Konfigurace spolupracujících systémů (MDM, Active Directory a další)
- Dodavatel připraví podrobné akceptační testy WAF
- Dodavatel provede pod dohledem Zákazníka akceptační testy WAF
- Dodavatel provede analýzu stávajících procesů zákazníka a připraví:
    - Soupis procesů, dotčených implementací WAF
    - Soupis rolí v rámci dotčených procesů
    - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
    - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
    - Přiřazení rolí k jednotlivým procesním krokům
- Dodavatel proškolí zástupce Zákazníka v:
    - Řešení a základní operativě
    - Upravených procesech
- Dodavatel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Druhá část - Specifikace implementačního procesu a požadovaných produktů a výstupů řešení ADC

- Dodavatel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie ADC, jejíž obsah bude následující:
    - Popis terminologie, použité v dokumentu
    - Informace o stávajícím prostředí Zákazníka
    - Seznam aplikací, které budou ADC využívat
    - High-level popis řešení
    - Popis změny v infrastruktuře
    - Řešení autentizace administrátorů ADC protokolem TACACS+
- Dodavatel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
    - Vymezení rozsahu řešení
    - Popis funkčních vlastností požadovaného zabezpečení aplikací technologií ADC
    - Popis úprav existujícího IT prostředí Zákazníka
    - Popis cílové úpravy vnitřních procesů
- Dodavatel vytvoří Low Level Design s následujícím obsahem:
    - Celkový návrh řešení ADC
    - Typizované konfigurační šablony (soubor pravidel) pro řízení aplikačního provozu
    - Jmennou konvenci pro ADC řešení
    - Konfigurace ADC clusteru
    - Konfigurace politik řízení aplikačního provozu pro aplikace
    - Vytvoření a implementace standardů (soubor pravidel) pro SSL terminaci
    - Vytvoření a implementace standardů (soubor pravidel) pro monitoring aplikací
    - Vytvoření a implementace standardů (soubor pravidel) pro manipulaci s HTTP provozem (vkládání odebíraní HTTP záhlaví apod.)
    - Vytvoření a implementace standardů pro optimalizaci TCP a HTTP provozu
    - Konfigurace ochrany proti DoS a DDoS aplikačním útokům
    - Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace
    - Konfigurace spolupracujících systémů (MDM, Active Directory a další)
- Dodavatel ve spolupráci se Zákazníkem vytvoří plán scénářů vysoké dostupnosti aplikací
- Dodavatel připraví podrobné akceptační testy ADC
- Dodavatel provede pod dohledem Zákazníka akceptační testy ADC
- Dodavatel provede analýzu stávajících procesů zákazníka a připraví:
    - Soupis procesů, dotčených implementací ADC
    - Soupis rolí v rámci dotčených procesů
    - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
    - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
    - Přiřazení rolí k jednotlivým procesním krokům
- Dodavatel proškolí zástupce Zákazníka v:
    - Řešení a základní operativě
    - Upravených procesech
- Dodavatel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Příloha č. 2 Smlouvy

Druhá etapa

Technická a implementační specifikace

Popis požadovaného řešení

Objednatel požaduje dodávku dvojice zařízení webové proxy s centrálním managementem pro zajištění funkčních požadavků v oblasti webové bezpečnosti, který zajistí požadovanou službu a zvýší úroveň ochrany vnitřní sítě proti možným hrozbám obsaženým uvnitř webové komunikace.

Kontrola webové komunikace je vyžadována zejména v těchto základních oblastech:

- Možnost filtrace prohlížení nevhodného obsahu
- Možnost ochrany proti komunikaci obsahující zavirovaný obsah
- Možnost ochrany proti komunikaci obsahující malware
- Možnost autentizace uživatelů komunikujících přes webovou proxy
- Možnost aplikační kontroly komunikující přes http a https protokol
- Možnost kontroly https protokolu (dekrypce HTTPS)
- Možnost omezení šířky pásma pro streamované aplikace
- Možnost centrálního monitoringu a reportingu webového provozu
- Možnost centrální správy a konfigurace politik
- Možnost nasazení webových proxy ve vysoké dostupnosti

Součástí dodávky musí být i případné licence a to v počtu pro 700 uživatelů.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s aktuální verzí VKB.

- Řízení provozu
- Autentizace uživatelů a správců systému
- Logovaní
- Autorizace uživatelů a správců systému
- Použité šifrovací a hashovací algoritmy
- Vysoká dostupnost
- Atd.

Dále musí být provedena iniciální konfigurace a případná registrace licencí.

Technická specifikace zařízení a SW

Požadavky na celkové řešení webové proxy
Řešení musí být plně redundantní
Řešení musí podporovat centralizovanou konfiguraci pomocí dedikované management appliance
Řešení musí podporovat balancování
Řešení musí poskytnout podporu na HW, licence a SW po dobu 5 let
Řešení musí být jednoduše škálovatelné pro případ rozšíření
Řešení musí být výkonově dimenzováno na 1000 uživatelů a licencováno na 700 uživatelů

Jedno fyzické zařízení musí být schopné zpracovat minimálně 650 požadavků za sekundu při zapnutých všech bezpečnostních funkcích (NTLM ověřování uživatelů, HTTPS dešifrování, antivirus, antimalware, filtrování URL, proxy cache)
Malware kontrola a filtrování
Spyware/Adware/obecná ochrana proti webovým hrozbám
Antivirová ochrana
Automatická aktualizace všech antimalware signatur po 5 minutách nebo častěji
Podpora současného provozu více antimalware engines přímo na sobě (ne na dalším serveru)
AV engines
Ochrana proti phishing útokům
Automatická aktualizace pravidel na ochranu proti phishing útokům
Podpora filtrování URL
Minimálně 60 URL kategorií
Používané databáze pro URL/web filtrování
Vytváření politik per identita/uživatel
Definice politik dle časového okna
Definice politik dle URL kategorie
Definice politik pro cílové URL
Definice politik pro cílovou IP adresu
Možnost blokování
Možnost pouze monitorovat
Možnost zobrazit notifikační stránku při přístupu s možností potvrzení sdělení a vytvoření záznamu v logu
Možnost vytvoření vlastních URL kategorií
Kategorizace URL (domén) i vyšších řádů (subdomén)
Možnost filtrovat přístup na Webmail
Možnost filtrovat přístup na web chat aplikace
Dynamická kategorizace nekategorizovaných URL přímo na zařízení
Dynamická kategorizace nekategorizovaných URL v cloud výrobce
Filtrování na základě web reputace
Nastavitelné reputační filtrování na základě hodnoty reputace pro blokování/povolení/skenování obsahu
Blokování metody HTTP POST pomocí metadata (file type, file name, file size)
Plnohodnotné a pravdivé skenování obsahu pro detekci typu souboru
Skenování na vrstvě TCP pro detekci nakažených stanic s aplikacemi, které komunikují po nestandardních portech
Monitorování a blokování malware spojení na všech 65535 portech
Monitorování a blokování malware spojení v příchozím i odchozím směru
Proxy cache a výkon
Kapacita proxy cache minimálně 500 GB (v RAID)
Maximální velikost cacheovaného objektu alespoň 1 GB
Technologie proxy cache
Implementace v transparentním módu pomocí WCCPv2
Implementace v transparentním módu pomocí policy routingu nebo L4 přepínače
Implementace jako explicitní proxy
Implementace jako explicitní proxy pomocí PAC souboru anebo WPAD
Možnost hostování PAC souborů přímo na řešení

Podpora více upstream proxy s podmíněným směrováním HTTP provozu
Více datových portů pro skenování web provozu
Možnost současného provozu řešení v explicitním i transparentním módu
Kontrola protokolů pro kontrolu
HTTP
HTTPS (dešifrování provozu)
FTP over HTTP
FTP (native)
Filtrování dílčích elementů web stránek
Filtrování konkrétních typů prohlížečů a jejich verzí
Blokování Java
Blokování ActiveX
Detekované typy archivů
Detekce vnořených archivů
Blokování konkrétních typů souborů
Detekce a blokování šifrovaných souborů
Blokování souborů nad definovanou maximální velikost
Monitorování a blokování aplikací P2P, IM, Youtube, Facebook, Flash video na aplikační úrovni (AVC)
Možnost omezení šířky pásma pro media streaming provoz (youtube, atd...)
Granulární rozpoznávání obsahu stránek facebook (tzn. Povolení přístupu na facebook, ale blokování facebook chat, facebook video či facebook games)
Ověřování uživatelů
Autorizace uživatele na základě IP adresy
Autorizace uživatele na základě subnetu
Ověření uživatele oproti LDAP (LDAPS)
Active directory ověření uživatele pomocí NTLMSSP (integrované ověřování Windows) - NTLMv1, NTLMv2
Podpora LDAP/Active directory skupin pro přiřazení politik
Pro NTLM podpora Windows serverů 2000/2003/2008/2012
Podpora Kerberos
Administrace a management
HTTPS Management console
CLI přístup pomocí SSH
RS232 serial console port
Podpora centralizovaného managementu (vytváření konfigurace na jednom místě a poté její automatická distribuce)
Ověřování a autorizace administrátorů pomocí RADIUS
Ověřování administrátorů pomocí lokálních účtů
Neomezený počet vlastních (administrátorem definovaných) URL kategorií
Správa uživatelskými účty s různými právy
Napojení do centrálního dohledu pomocí SNMP
Podpora centrálního logování pomocí SYSLOG
Hardware a podpora (v případě realizace řešení více appliance se uvedené požadavky vztahují na každou z nich)

řešení musí mít formu appliance s vlastním proprietárním operačním systémem
Podpora pro pět (5) GigabitEthernet rozhraní na hardware platformě
Více HDD v hardware RAID poli
Celková instalovaná disková kapacita minimálně 2,4 TB
32 GB RAM
CPU s multicore software podporou (alespoň 6 jader)
1U rack šasi
Poskytovaná podpora přímo od výrobce
Podpora výrobce formou email, telefon, web
Přístup na portál podpory výrobce a znalostní báze
Plná podpora hardware po dobu trvání kontraktu podpory
Reporting
GUI rozhraní pro účely administrace a prohlížení reportů
Možnost vlastního nastavení reportu
Možnost detailního prohlížení reportů pro každého uživatele a jeho aktivit pro účely analýzy
Export reportů a plánování jejich pravidelného zasílání
Zobrazení podezřelých aktivit pro každého uživatele
Top-N reporty pro: Top uživatele, top URL, top URL kategorie, top malware, používání web aplikací
Možnost ukládání reportu v PDF formátu

Požadavky na centrální management
Řešení musí poskytnout podporu na HW, licence a SW po dobu 5 let
Řešení musí být výkonově dimenzováno na 1000 web uživatelů. Licencováno na 700 web uživatelů
Jedno fyzické zařízení musí být schopné uchovat detailní data o každé transakci minimálně 3 měsíce zpětně bez použití externího uložiště při běžném provozu
Funkce Web Security Management a Reporting
Centralizovaná replikace konfigurace na více web security zařízení
Sdružování web security zařízení do skupin
Možnost delegace práv pro konfigurování pouze konkrétní politiky konkrétnímu administrátorovi
Správa web security zařízení s různými verzemi OS
Možnost skrýt nepřiřazené politiky pro delegovaného administrátora
Možnost zobrazit ostatní politiky pouze pro čtení pro delegovaného administrátora
Možnost plánování update politik na konkrétní čas
Centralizovaná kolekce dat od více web security zařízení
Vytváření konsolidovaných reportů z dat od více web security zařízení
Možnost sledování a dohledávání konkrétní transakce přes více web security zařízení pomocí jednoho GUI rozhraní
Vygenerování reportu on-demand o aktuální aktivitě daného uživatele
Historické ukládání reportů a dostupnosti reportovaných dat
Plánované reporty pro doručení
Administrace a management
HTTPS Management console
CLI přístup pomocí SSH

RS232 serial console port
Master administrator uživatel ověřován pomocí RADIUS/LDAP/MS AD
Administrátoři ověřováni pomocí lokálních účtů
Administrativní role pouze pro čtení
Možnost stateful backup všech web reportovaných dat na případném záložním management zařízení
Možnost plánování data backup
Hardware a podpora
Řešení musí mít formu appliance s vlastním proprietárním operačním systémem
Zařízení musí být i formou virtuálního appliance do Vmware z důvodu redundance (rozšíření počtu virtuálních strojů musí být bezplatné)
Více HDD v hardware RAID poli v RAID 10
Celková instalovaná disková kapacita minimálně 3,6 TB
16 GB RAM
Alespoň 2x Hexa-core CPU s multicore software podporou
Maximálně 1U rack šasi
Poskytovaná podpora přímo od výrobce
Podpora výrobce formou email, telefon, web
Přístup na portál podpory výrobce a znalostní báze
Plná podpora hardware po dobu trvání kontraktu podpory

Specifikace implementačního procesu a požadovaných produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie WEB proxy, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury WEB proxy a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, FW, AD, DHCP, DNS, CA, VPN gateway)
  - Identifikace tříd uživatelů a zařízení, specifikace přístupových politik
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis typu nasazení
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. PoC s následujícími kroky:
  - Instalace WEB proxy a zapojení do PoC infrastruktury
  - Integrace s potřebnou interní infrastrukturou (MS AD, CA, NTP, DNS, atd.)
  - Konfigurace a licencování
  - Nastavení politik dle funkční specifikace
  - Testování

- Zhotovitel připraví podrobné tzv. PoC akceptační testy
- Zhotovitel provede pod dohledem Objednatele PoC akceptační testy

Druhá část

- Zhotovitel vytvoří na základě úspěšně provedených akceptačních testů Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Typizované konfigurace jednotlivých typů přístupových politik
  - Konfigurace WEB proxy
  - Konfigurace spolupracujících systémů (FW, Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Třetí část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací WEB proxy
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Příloha č. 3 Smlouvy

Třetí etapa

Technická a implementační specifikace

Popis požadovaného řešení

Objednatel požaduje dodávku dvojice zařízení Next-Generation Firewall v redundantním režimu active-standby pro zajištění vysoké dostupnosti. NGFW bude zajišťovat segmentaci sítě, pokročilou analýzu provozu a filtrovaní provozu ve vnitřní síti OLK.

NGFW musí poskytovat funkcionalitu zejména v těchto základních oblastech:

- Oddělení sítí dle typu připojených zařízení – segmentace sítě a ochrana jednotlivých segmentů
- Filtrování provozu dle požadovaných komunikací
- Pokročilé inspekce protokolů (až do L7 ISO OSI)
- Prevence a detekce útoků na úrovni síťového provozu
- Ochrana proti Malware hrozbám s dynamickou analýzou (sandboxing)
- Možnost podpory URL filtrace
- Možnost využívání znalostní databáze výrobce pro blokaci nebezpečných zdrojů (nebezpečné IP adresy, URL nebo DNS domény v Internetu)
- Možnost centrálního managementu společného pro oba NGFW
- Možnost centralizovaného nastavení bezpečnostních politik
- Možnost centralizované distribuce nových verzí sw a aktualizací
- Management musí poskytovat správu a řízení uživatelů, jejich oprávnění a monitoring
- Zajištění podpory výrobce při řešení funkčních problémů

Součástí dodávky musí být i případné licence.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s platným a účinným zákonem o kybernetické bezepečnosti.

- Řízení provozu
- Autentizace uživatelů a správců systému
- Logování
- Autorizace uživatelů a správců systému
- Použité šifrovací a hashovací algoritmy
- Vysoká dostupnost
- Atd.

Dále musí být řešena iniciální konfigurace a registrace licencí NGFW.

Technická specifikace zařízení a SW

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

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Výkon a funkcionalita firewallu	
Formát zařízení	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	8
Možnost rozšíření o moduly rozhraní	2
Možnost rozšíření o další 10Gb SFP+ rozhraní	8
Možnost rozšíření o další 40Gb SFP+ rozhraní	4
Redundantní zdroje	-
Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.10M/4.5M
Rychlost vytváření nových spojení přes stavový FW	Min. 150K/s
Propustnost stavového firewallu (multiprotokolový režim)	Min. 10 Gbps
Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 12 Gbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	Min. 10 Gbps
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 4 Gbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 2.5 Gbps
VPN propustnost	Min. 8 Gbps
Současný počet VPN spojení (IPSec/SSL)	Min. 10.000
Podpora L2 (transparentního) módu s podporou NAT a PAT	-
Podpora L3 (routovaného) módu s podporou NAT a PAT	-
Podporovaný počet VLAN	Min. 1024
Podpora stateful failover	active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	-
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	-
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	-
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	-
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů	-
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	-
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	-
Podpora Policy based Routing	-
Podpora kontroly paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	-
Podpora filtrace IPv4, IPv6	-
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	-
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	-

Podpora inspekce IPv6 provozu	-
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	-
Podpora NAT64 a DNS64	-
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	-
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	-
Možnost rozšíření o funkce NextGen FW	-
Možnost rozšíření o funkce NextGen IPS	-
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	-
Zohlednění kontextových informací o koncovém zařízení (typ, stav, apod.) a využití ve filtrech	-
API rozhraní pro sdílení kontextových informací s dalšími systémy	-
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	-
Funkce IPS a anti-malware	
Možnost definovat typ provozu předávaný k inspekci do IPS	-
Podpora také IDS režimu – pasivního monitorování (TAP režim)	-
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	-
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	-
Podpora 802.1Q tagovaných rámců	-
Podpora různých IPS politik pro různé typy provozu	-
Inspekce pro IPv4 i IPv6	-
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	-
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	-
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	-
Podpora aplikace pro psaní zákaznických filtrů	-
Podpora importu komunitních filtrů/signatur Snort	-
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	-
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	-
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host" jako je spyware, phishing nebo Botnet C&C	-
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře Objednatele, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	-
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	-
Možnost vyhledávání typu signatury v centrální databázi výrobců podle typu a závažnosti útoku	-
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	-
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	-
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	-
Možnost definice uživatelské vrstvy politik	-

Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	-
Různé politiky lze sdílet a aplikovat na různé senzory	-
Podpora aktivní online ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV výrobců	-
Ochrana před malware typu „zero day attack" které nelze detekovat tradičními antiviry	-
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	-
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	-
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	-
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru výrobce jako malware je na koncových stanicích okamžitě přesunut do karantény	-
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	-
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	-
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation"	-
Možnost automatické i manuální klasifikace stanice jako "kritické" se zohledněním v pravidlech, reportech apod.	-
Podpora „remediation" modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	-
Otevřené rozhraní pro uživatelsky vytvářené „remediation" moduly	-
Podpora databází reputací adres v Internetu (Security Intelligence)	-
Funkce Next-Gen FW	
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	-
Podpora pasivního monitorování (TAP režim)	-
Podpora 802.1Q tagovaných rámců	-
Podporovaných aplikací	Min. 3000
Kategorie aplikací (nebezpečné, důležité, apod.)	-
Filtrace podle typů aplikací webových i ne-webových	-
Filtrace podle reputace serverů	-
SSL inspekce (dekrypce/enkrypce)	-
Security Inteligence database – známé uzly botnet sítí C&C	-
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	-
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	-
Možnost integrovat vlastní reputační databáze	-
Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)	-
Filtry mohou zohlednit roli a identitu uživatele	-
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	-
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	-
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení Operační systém

	Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti
Přehled o síťových spojeních má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact" aplikace Množství přenesených dat
Správa	
Vzdálená správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	-
Přístup ke GUI http/https protokolem	-
Možnost vzdáleného přístupem protokolem ssh přímo do FW	-
Možnost přístupu k textovým logům (syslog) přímo ve FW	-
Možnost centrální správy při nasazení více firewallů	-
Při centrální správě: možnost sdílených bezpečnostních politik	-
Při použití clusteru se spravuje pouze jeden logický prvek	-
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	-
Zobrazení logů a událostí v grafickém rozhraní správy	-
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	-
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	-
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	-
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	-

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

Specifikace implementačního procesu a požadovaných produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie NGFW, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury NGFW a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, AD, DHCP, DNS, CA, atd.)
  - Identifikace tříd uživatelů a zařízení, specifikace komunikační matice
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis implementovaných funkcí
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel vytvoří Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Konfigurace NGFW
  - Požadavky pro konfigurace spolupracujících systémů (Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Druhá část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací NGFW
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Příloha č. 4 Smlouvy

Čtvrtá etapa

Technická a implementační specifikace

High-level popis požadovaného řešení

Stávající stav

Síť KÚOK je vybavena na přístupové vrstvě přepínači Cisco, řady Catalyst 2960 (WS-C2960X-48TD-L) a C4510R. WiFi síť je postavená na bázi Cisco WLC AIR-CT2504 a AP řad CAP702, AP1131, CAP1552EU a CAP1602. Jako VPN koncentrátor slouží firewall ASA 5585.

Počty zařízení a klientů jsou následující:

Typ zařízení	Počet aktuálně	Počet s výhledem
AP	8	14
WLC	1	2
Přepínače	26	30
IP telefon	10	10
Tiskárny	70	85
Ostatní pasivní zařízení	17	30
Pracovní stanice	536	600
Notebook	203	250
Zařízení externistů/dodavatelů	70	90
Mobilní telefony	236	270
Tablety	79	100
VPN gateway	2	2

Základem autentizace a autorizace v síti je doména s 2 řadiči Active Directory. Tyto uzly současně realizují certifikační autoritu. Certifikační autorita vydává certifikáty stanicím pro přihlášení do interní WiFi. Záplaty jsou na stanice distribuovány pomocí WSUS serverů a SW je instalován a vzdálená podpora je poskytována z Microsoft SCCM serveru. DHCP služby jsou poskytovány z dedikovaného serveru.

V rámci jiného výběrového řízení bude implementován systém MDM, který bude spravovat mobilní zařízení interních uživatelů.

Požadavky na řešení

Objednatel požaduje dodání redundantního autentizačního systému pro autentizaci zařízení a uživatelů v LAN a WiFi prostřednictvím protokolu 802.1X a zařízení a uživatelů, přistupujících vzdáleně do sítě Objednatele prostřednictvím VPN. Přístup bude sjednocen na stejnou úroveň oprávnění ve všech třech přístupových technologiích. Mimo interních a externích uživatelů bude autentizační systém ověřovat i Guest uživatele pomocí stávajícího portálu na bezdrátovém kontroléru a musí disponovat vlastnostmi pro onboarding privátních i firemních mobilních zařízení.

Autentizační systém bude ověřovat i přístup administrátorů na síťové prvky protokolem RADIUS a TACACS+, včetně autorizace oprávnění administrátorů na jednotlivých prvcích.

Mezi očekávané přínosy patří:

1. zabezpečení přístupu s možností karantény zařízení, která neodpovídají politice
2. zjednodušení konfigurace přepínačů
3. podpora mobility uživatelů
4. snadnější segmentace podle rolí uživatelů a snadnější vynucení přístupových oprávnění na prvcích, chránících datacentrum.

Autentizační systém musí být schopen nativního začlenění do existující MS domény, ve které bude ověřovat interní uživatele protokolem Kerberos a ze které bude získávat podklady pro autorizaci uživatelů a zařízení. Autentizace doménových stanic a uživatelů musí být zajištěna takovým mechanismem, že se v jednom kroku ověří jak stanice, tak i uživatelé, obojí protokolem 802.1X. Pouze v případě, že se úspěšně ověří jak stanice, tak i uživatel, bude povolen přístup do sítě. Rámcové požadavky na autentizaci jsou uvedeny v tabulce níže. Systém musí být schopen zajistit bezproblémový provoz uživatelské autentizace na bázi uživatelského jména a hesla současně s uživatelskými certifikáty.

Autentizační systém musí být schopen ověřit zdraví Windows pracovních stanic a podle výsledku autorizovat stanici do karantény nebo do produkční VLAN. Karanténa musí být realizovatelná jako karanténní VLAN nebo přístup omezený pomocí ACL. Autentizační systém musí být současně schopen spolupracovat se systémy MDM a SCCM v rámci autorizačních rozhodnutí. Z obou systémů musí být schopen získat informaci o stavu zařízení, resp. jeho shodě s požadovanou politikou. Zdraví stanic musí být periodicky ověřovatelné a v případě, že stanice nebude v souladu s požadavky, musí systém umožnit uvedení stanice do souladu pomocí „wizardu", který uživatele procesem povede.

Rámcová autentizační matice pro LAN a WiFi

Uživatel/zařízení	**Interní uživatel**	**Externí uživatel s účtem v doméně**	**Externí uživatel bez účtu v doméně (servisní technik)**	**Guest**	**Autentizace zařízení**
Doménová stanice	ověření stanice+ověření uživatele (U/P+CERT) Posture/SCCM kontrola	ověření stanice+ověření uživatele (U/P+CERT) Posture/SCCM kontrola	x	x	certifikát zařízení
Doménový notebook	ověření stanice+ověření uživatele (U/P+CERT) Posture/SCCM kontrola	ověření stanice+ověření uživatele (U/P+C Posture/SCCM kontrola ERT)	x	x	certifikát zařízení
Pracovní stanice mimo doménu	x	x	MAC adresa	Guest portál a U/P	
Zařízení bez 802.1X suplikanta	x	x	x	x	MAC adresa
Mobilní zařízení pod MDM	jen autentizace zařízení	jen autentizace zařízení	x	x	certifikát zařízení ověření v MDM
Mobilní zařízení mimo MDM	x	x	x	Guest portál a U/P	x

Rámcová autentizační matice pro VPN

Uživatel/zařízení	Interní uživatel	Externí uživatel s účtem v doméně	Externí uživatel bez účtu v doméně (servisní technik)
Doménový notebook	ověření uživatele (U/P+CERT) Posture/SCCM kontrola	x	x
Pracovní stanice mimo doménu	x	ověření uživatele (U/P+CERT) Posture kontrola	x
Mobilní zařízení pod MDM	ověření uživatele (U/P+CERT)	x	x
Mobilní zařízení mimo MDM	x	x	x

Autentizační systém musí být, samostatně nebo ve spojení s jiným integrovaným SW systémem, schopen nabídnout následující vlastnosti pro začlenění do stávajících technických procesů:

1. autorizace operací založená na rolích
2. autorizace registrace MAC adres do skupin založená na rolích
3. disponuje připravenými workflow pro registraci MAC adres pro pasivní zařízení, externisty, pro případ selhání 802.1X autentizace na stanicích, re-image, blacklisting a další
4. umožňuje full-text prohledávání databáze MAC adres
5. automatická expirace registrované MAC adresy ke stanovenému času a jejich automatické mazání z databáze autentizačního systému
6. prezentace aktuálních i historických autentizačních relací, jejich stavu a detailu autentizačních relací z autentizačního systému
7. možnost náhledu na atributy uživatelských účtů v Active Directory
8. možnost náhledu na konfiguraci portů přepínačů
9. možnost náhledu na stav autentizace z pohledu přepínačů
10. možnost black-listingu zařízení s jejich okamžitým odpojením od sítě

Autentizační systém nebo jeho doplňková SW komponenta musí být schopna zabezpečit WoL v prostředí se změnou VLAN mezi autentizací stanice a uživatele.

Systém musí být výkonnostně dimenzován pro autentizaci zhruba 2000 koncových zařízení (včetně uživatelských stanic, mobilních zařízení a Guest uživatelů) a administrátorů na cca. 50 síťových zařízení.

Zhotovitel zajistí potřebné licence v odpovídajícím počtu.

Technická specifikace zařízení a SW

Požadovaná funkcionalita/vlastnost
Obecná charakteristika ověřovacího řešení
Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.)
Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1X) a pro VPN přístup
Poskytuje AAA funkce (viz níže)

Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)
Je dostupné ve formě Virtuálního stroje na platformách Vmware, Linux KVM a Microsoft Hyper-V
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)
Podporované protokoly
RADIUS pro autentizaci, autorizaci, zaznamenávání
Proxy funkce pro externí RADIUS
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST
Podpora TACACS+ pro centrální řízení administrativního přístupu na síťová zařízení
Podporované databáze uživatelů (s možností definovat pořadí průchodu)
Interní (pro uživatele i koncová zařízení)
Podpora více nezávislých Active Directory
LDAP (RFC 2251)
RADIUS Token indentity source (RFC 2865)
RSA RADIUS token server
Certifikační profil
Ověřování uživatelů a zařízení
Ověření uživatelů/zařízení heslem nebo certifikátem
Ověření MAC adresou připojovaného zařízení
Autorizace: pružný systém pro definici pravidel pro přístup k síti
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:
uživatele (role, skupiny)
stavu a typu koncového zařízení (viz níže)
místa připojení
historie připojení
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě
Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“
Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti
Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)
Accounting
Zaznamenávání aktivity uživatelů a zařízení připojených k síti
Dotazovací systém, korelace záznamů, centralizované výkazy
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)
Funkce GUEST serveru
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi
Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů
Samoobslužný portál pro uživatele
Ověření přes HTTP a HTTPS
Propojení se SMS bránou pro zasílání Guest účtu

Propojení s email serverem pro zasílání Guest účtu
Rozpoznávání typu koncových zařízení
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)
Předdefinované profily pro síťová zařízení NAD od různých vendorů
Podpora pro IPv6 koncová zařízení
Podpora BYOD
Onboarding (registrace, provisioning, nastavení klientských zařízení)
Onboarding/provisioning proces formou samoobsluhy
Specifické politiky pro BYOD zařízení
Možnost nastavení limitu BYOD zařízení pro jednoho uživatele
Interní CA, pro vydávání certifikátů BYOD zařízením
Interní CA lze řetězit jako subordinate pod firemní CA
Podpora MDM
Workflow pro registrace do MDM
Výměna informací z MDM platformy a využití v politikách (např. pokud zařízení je „compliant")
Ovládání MDM přímo z prostředků bezpečnostního managementu (zamykání, mazání, apod.) zařízení
Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení)
Rozpoznávání stavu koncových zařízení a jeho náprava
Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat:
instalovaný operační systém
opravy instalované v operačním systému
hodnoty položek v registry databázi systémů Windows
stav aplikací, zejména antivirů, antispyware, antimalware a firewall
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)
Varianta agentů s GUI i bez GUI
Další vlastnosti
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)
Podpora SXP (Exchange Protocol) dle IETF
Otevřené API pro podporu propojení se zařízeními třetích stran
Distribuce identitních informací na další bezpečnostní síťové prvky, které ji budou využívat pro zajištění jejich vlastní funkčnosti (webová proxy, NGIPS, ...)
Podpora komunikace s Microsoft SCCM pro zjištění stavu zařízení z pohledu SW záplat a instalovaného SW.
Rozhraní nebo externí aplikace pro centralizovanou správu MAC adres a provozní troubleshooting s následujícími vlastnostmi
Autorizace operací založená na rolích, definovaných v AD
Autorizace registrace MAC adres do skupin založená na rolích, definovaných v AD
Disponuje připravenými workflow pro registraci MAC adres pro pasivní zařízení externisty, pro případ selhání 802.1X autentizace na stanicích, re-image, blacklisting a další
Umožňuje full-text prohledávání databáze MAC adres a auditování provedených operací
Registrace MAC adres a automatická expirace registrované MAC adresy ke stanovenému času a jejich automatické mazání z databáze
Prezentace aktuálních i historických autentizačních sessions, jejich stavu a detailu autentizační session
Možnost náhledu na atributy uživatelských účtů v Active Directory
Možnost náhledu na konfiguraci portů přepínačů
Možnost náhledu na stav autentizace z pohledu přepínačů
Umožňuje operace provádět prostřednictvím REST API
Funkce pro správu ověřovacího systému

Centralizovaná správa
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému
Zjednodušení správy vytvářením skupin uživatelů, koncových a síťových zařízení
Grafické rozhraní pro definici pravidel přístupu k síti
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)
Zaznamenávání událostí na externí syslog server
Podpora SNMPv3
NTP pro synchronizaci času
SMTP pro zasílání zpráv a výstrah přes e-mail

Specifikace implementačního procesu a požadovaných produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie 802.1X, autentizace administrátorů na síťové prvky a autentizace do VPN, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury přístupových technologií, zahrnutých do řešení a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, VPN, AD, DHCP, DNS, CA, VPN gateway)
  - Identifikace tříd uživatelů a zařízení, specifikace autentizačních scénářů
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů na síťové prvky protokolem TACACS+
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis autentizačních scénářů
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. PoC s následujícími kroky:
  - Instalace Cisco ISE a zapojení do PoC infrastruktury
  - Integrace s Cisco WLC nastavení politik dle funkční specifikace
  - Konfigurace WLC pro 802.1X a definované scénáře
  - Nastavení Cisco ISE
  - Integrace Cisco ISE s MDM
  - Konfigurace autentizačních, autorizačních, profilačních a posture politik
  - Konfigurace a otestování nativních suplikantů a Anyconnect klienta
  - Vytvoření zadání pro instalaci a konfiguraci aplikací pro centrální správu MAC adres a pro provozní troubleshooting 802.1X řešení,
  - Instalace a konfigurace aplikací pro centrální správu MAC adres a pro provozní troubleshooting 802.1X řešení,
  - Testování autentizačních scénářů
  - Konfigurace Guest řešení
  - Konfigurace VPN řešení
  - Konfigurace vzorových síťových prvků pro autentizaci, autorizaci a accounting přístupu administrátorů

- Zhotovitel připraví podrobné tzv. PoC akceptační testy
- Zhotovitel provede pod dohledem Objednatele PoC akceptační testy

Druhá část

- Zhotovitel vytvoří na základě úspěšně provedených akceptačních testů Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Typizované konfigurace jednotlivých typů síťových prvků
  - Konfigurace Cisco ISE
  - Konfigurace suplikantů
  - Konfigurace aplikací pro centrální správu MAC adres a pro provozní troubleshooting
  - Konfigurace spolupracujících systémů (MDM, Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Třetí část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací 802.1X, autentizace administrátorů a přístupu do VPN
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Příloha č. 5 Smlouvy

Pátá etapa

Technická a implementační specifikace

Popis požadovaného řešení

Objednatel požaduje dodávku zařízení (HW nebo virtuální appliance) pro zajištění funkčních požadavků v oblasti Enterprise Mobility Managementu - EMM, který zajistí požadovanou službu a podporu automatizace nastavení mobilních zařízení, distribuce firemních mobilních aplikací, certifikátů, konfigurací a profilů.

Řízení mobilních zařízení je nutné zejména v těchto základních oblastech:

- řízení a správa povolených přístupů do vnitřní sítě
- centralizované nastavení bezpečnostních politik
- zajištění bezpečnosti firemních dat, dokumentů a přístupu k nim (aktualizace, vynucení politik, blokace, výmaz dat)
- centralizace dohledu připojených mobilních zařízení do sítě
- řízená distribuce mobilních aplikací
- centralizovaná distribuce bezpečnostních certifikátů
- podpora instalace, aktualizace a nastavení zařízení a aplikací
- správa a řízení uživatelů, oprávnění, restrikce, monitoring
- možná podpora uživatele při problémech se zařízením/aplikací

Součástí dodávky musí být i případné licence a to v počtu pro 200 mobilních zařízení.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s platným a účinným zákonem o kybernetické bezpečnosti.

- Řízení provozu
- Autentizace uživatelů a správců systému
- Logovaní
- Autorizace uživatelů a správců systému
- Použité šifrovací a hashovací algoritmy
- Vysoká dostupnost
- Atd.

Dále musí být řešena iniciální konfigurace (autokonfigurace) a registrace připojeného mobilního zařízení. Řešení musí umožňovat kromě registrace nového mobilního zařízení administrátorem i možnost registrace nového mobilního zařízení samotným uživatelem a automatické přiřazení bezpečnostních politik.

Technická specifikace zařízení a SW

Funkční požadavky
Automaticky omezuje přístup k EMM na počet mobilních zařízení vázaných na jednoho zaměstnance/uživatele.
EMM kompatibilita. • Vyžadováno mobilní OS: Android, iOS, Windows 10

Zhotovitel zajistí pravidelné aktualizace EMM o podporu aktualizovaných OS a nových typů mobilních zařízení dle aktuálních trendů na trhu mobilních zařízení.
EMM Bezpečnost
Centralizované a vynucené nastavení bezpečnostních politik na mobilních zařízeních před tím než je na zařízení možno přistupovat k firemním aplikacím a datům a do firemní sítě.
Možnost validace OS mobilního zařízení a jeho kompatibilita s vyžadovanými bezpečnostními politikami.
Možnost vyhodnotit mobilní zařízení, kde bylo manipulováno s OS zařízení (jailbrake devices, rooted devices).
Možnost vynucení PIN/PASSWORD na mobilním zařízení.
Možnost vynucení automatického zamykání při neaktivitě.
Podpora uživatelské autorizace přes interní certifikáty.
Možnost white list / black list mobilního zařízení.
Interoperabilita s wifi infrastrukturou pro řízení přístupu mobilních zařízení do wifi sítě pro: • On-boarding ... automatizovaný proces nastavení zařízení pro přístup do sítě – generování/distribuce certifikátu. • Profiling ... nastavení bezpečnostních profilů a oprávnění přístupů do sítě. • Posture ... ověření stavu, zdali zařízení smí být připojeno do příslušné sítě.
Možnost vytvoření dedikované oblasti pro firemní aplikace a data se zabezpečením (zabezpečený kontejner). Pro oddělení soukromých a privátních dat, tzv. vytvoření samostatné zabezpečené oblasti na mobilním zařízení pro uložení firemních mobilních aplikací, firemních dat a certifikátů. Možnost zabránit kopírovat data mimo dedikovaný kontejner pro firemní data.
Podpora technologií Samsung Knox a Android for Work.
Možnost online blokovat přístup mobilnímu zařízení k firemním zdrojům (email, file share, atd.) v případě nesplnění bezpečnostních požadavků na mobilní zařízení.
Podpora vzdáleného smazání mobilního zařízení, které je řízeno bezpečnostní politikou z EMM.
Možnost napojení na centralizovaný dohled. Možnost odesílání logů do externího systému (SIEM/syslog sever).
EMM SW Inventory
Možnost nastavit automatickou distribuci firemních mobilních aplikací na cílové mobilní zařízení pomocí jednotlivých profilů řízených v EMM. Zajištění Centralizované správy firemních aplikací a přístupů na mobilním zařízení.
Možnost vzdálené obnovy aplikační vrstvy na cílovém zařízení z centrálního úložiště firemních mobilních aplikací.
Podpora centralizované správy mobilního zařízení za použití interní evidence (IMEI, SIM) s vazbou na profil mobilních zařízení řízených pomocí EMM.
Podpora pro řízenou distribuci aktualizací firemních mobilních aplikací, certifikátů a oprávnění na mobilní zařízení podle profilu.
Součástí EMM je vlastní Store pro uložení firemních mobilních aplikací. Možnost omezit dostupnost aplikací pro instalaci na firemní mobilní zařízení v rámci oficiálních application store – Google Play, Apple Store, Microsoft.
EMM podpora SSO a interních autorizačních credentials poskytovaných Microsoft AD.
Podpora selective wipe, tedy možnost vzdáleného smazání centrálně distribuovaných aplikací z EMM.
Možnost vytváření whitelist a blacklist seznamů pro mobilní aplikace a následné využití těchto seznamů v bezpečnostních politikách pro řízení přístupu mobilních zařízení k firemním prostředkům.

Požadované možnosti nasazení EMM

On-Premise:

- HW appliance
- Virtuální appliance s podporou VMWare a Hyper-V

Specifikace implementačního procesu a požadovaných produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie EMM, správa mobilních zařízení a řízení přístupu mobilních zařízení k firemním prostředkům a datům, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury EMM a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, FW, AD, DHCP, DNS, CA, VPN gateway)
  - Identifikace tříd uživatelů a zařízení, specifikace registračních scénářů
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis registračních scénářů
  - Popis profilů pro jednotlivé mobilní OS
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. PoC s následujícími kroky:
  - Instalace EMM a zapojení do PoC infrastruktury
  - Integrace s potřebnou interní infrastrukturou (MS AD, CA, NTP, DNS, atd.)
  - Nastavení politik dle funkční specifikace
  - Konfigurace, registrace a otestování vybraných mobilních zařízení
  - Vytvoření zadání pro instalaci a konfiguraci aplikací pod centrální správou
  - Instalace a konfigurace aplikací pod centrální správou EMM
  - Testování scénářů přístupu pomocí mobilních zařízení
- Zhotovitel připraví podrobné tzv. PoC akceptační testy
- Zhotovitel provede pod dohledem Objednatele PoC akceptační testy

Druhá část

- Zhotovitel vytvoří na základě úspěšně provedených akceptačních testů Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Typizované konfigurace jednotlivých typů využívaných mobilních OS
  - Konfigurace EMM
  - Registrace mobilních zařízení
  - Konfigurace aplikací pod centrální správou
  - Konfigurace spolupracujících systémů (FW, Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Třetí část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací EMM
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Příloha č. 6 Smlouvy

Penetrační testy

Po ukončení implementace a kompletním odladění všech dílčích systémů zajistí Zhotovitel před zahájením ostrého provozu u nezávislého třetího subjektu provedení nezávislého penetračního testu sítě Objednatele, včetně jeho vyhodnocení v podobě reportu, který Zhotovitel předá Objednateli.

Zajištění penetračního testu zahrnuje povinnost připravit detailní penetrační testy a získat souhlas Objednatele s jejich obsahem.

Na základě výsledku penetračního testu a reportu provede Zhotovitel potřebné úpravy jednotlivých funkcionalit, nebo procesů. V takovém případě bude penetrační test opakován, a to do chvíle než bude výsledek penetračního testu úspěšný.

Po úspěšném dokončení penetračních testů upraví Zhotovitel Předávací dokumentaci připravenou v rámci jednotlivých etap Díla tak, aby odpovídala finálnímu nastavení jednotlivých komponent řešení a procesů po úspěšném dokončení penetračních testů a předá ji Objednateli. O předání Předávací dokumentace podepíší Smluvní strany protokol.

Příloha č. 7 Smlouvy

Podrobná technická specifikace nabízeného hardwaru a softwaru

PRVNÍ ETAPA - WEB APLIKAČNÍ FIREWALL

Technická a implementační specifikace

High-level popis nabízeného řešení

Webové aplikace publikované do vnějších sítí, zejména veřejné sítě Internet, mohou být náchylné na zranitelnosti vůči kybernetickým útokům a aplikačním DoS a DDoS útokům. Nasazením webového aplikačního firewallu (WAF) je možné provádět inspekci webové komunikace a ochranu před kybernetickými útoky. Zároveň je nutné zajistit vysokou dostupnost, rozklad zátěže - loadbalancing a funkci Reverzního proxy serveru aplikací prostřednictvím komponenty Application Delivery Controller (ADC).
Nabízíme dvojici HW zařízení v roli WAF a ADC. Dvojice HW řešení WAF a ADC bude publikovat definované služby, oddělovat reálné servery od přistupujících uživatelů, modifikovat a provádět inspekci webového provozu. Pokud zařízení neumožňuje integrovat obě funkcionality, bude dodáno jako separátní dvojice WAF zařízení a separátní dvojice ADC.
Řešení bude koncipované jako redundantní a vysoce dostupný cluster a bude fungovat v režimu Active-Active nebo Active-Standby. Řešení bude odpovědné za monitoring dostupných aplikací služeb, řízení distribuce a zátěže aplikačního provozu mezi servery, které budou jednotlivé aplikace a služby poskytovat. Řešení bude také zodpovědné za optimalizaci a modifikaci aplikačního provozu s cílem efektivně využívat zdroje aplikace nebo zamezit nežádoucí distribuci dat k uživatelům (např. manipulace s HTTP záhlavím, HTML kódem apod. šifrování cookies apod.). Řešení bude také zodpovědné za optimalizaci TCP provozu, HTTP kompresi a související optimalizaci aplikačního provozu.
Implementaci politik a pravidel pro řízení aplikačního garantujeme minimálně v rozsahu:

- Zapojení a integrace v prostředí Zákazníka
- Vytvoření HA clusteru
- Monitoring zdraví aplikací a služeb
- SSL terminace, management SSL certifikátů
- Napojení na monitorovací a logovací nástroje
- Reverzní proxy s funkcí NAT44, případně NAT 46, NAT 64
- Optimalizace HTTP provozu (HTTP komprese)
- Zabezpečení HTTP provozu (cookies, manipulace s HTTP záhlavím apod.)

Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu. Součástí těchto základních bezpečnostních politik je implementace dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem. Nabízený WAF obsahuje technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní vyhledávače Googlebot, Seznambot apod.). WAF také zajistí ochranu před únosy HTTP relací. WAF podporuje SSL terminaci, jelikož HTTP protokol bude šifrován.

Řešení musí být realizováno ve vysoké dostupnosti v režimu minimálně "active-standby".
Implementace bezpečnostních politik bude minimálně v rozsahu:

- Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.)

- Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10
- Ochrana proti manipulaci s cookies
- Ochrana parametrů webové aplikace
- Session Management – ochrana proti únosům relací
- Brute Force Ochrana – ochrana před prolomení hrubou silou
- Detekce robotických uživatelů aplikace u vybraných aplikací

Ostatní nabízené funkcionality webového aplikačního firewallu jsou uvedeny v tabulce technické specifikace. V případě integrace funkce WAF s funkcí ADC v jednom HW zařízení je přípustné, že požadavky na propustnost L4, L7, SSL a fyzické připojení budou splněny v pouze tomto jednom zařízení.

Technická specifikace nabízeného zařízení a SW

Technická specifikace řešení WAF

Pol. č.	Technické specifikace nabízeného řešení - WAF
1	2 ks samostatného HW zařízení s montáží do technologické 19" skříně (RACK), max. 2U nebo jako rozšiřující licence k ADC
2	V případě samostatného HW zařízení WAF plně redundantní napájecí zdroj AC
3	V případě samostatného HW zařízení WAF požadujeme min. 6x 1Gbps optických Ethernet rozhraní nebo slotů a zároveň min. 4 x 10 Gbps optických rozhraní nebo slotů pro Ethernet
4	V případě samostatného HW zařízení WAF, které obsahuje sloty pro optická rozhraní, nabízíme celkem 4x Ethernet moduly s podporou rychlosti 10 Gbps s vlnovou délkou 850 nm pro vlákno MMF (50/125)
5	V případě samostatného HW zařízení WAF Lights-out management - nezávislý servisní procesor pro vzdálenou správu zařízení (vypnutí/zapnutí zařízení, konzolový přístup)
6	L4 propustnost každého HW zařízení minimálně 18 Gbps
7	L7 propustnost každého HW zařízení minimálně 18 Gbps
8	Každé HW zařízení podporuje minimálně 425 000 L4 spojení za sekundu
9	Každé HW zařízení podporuje minimálně 20 milionů současných TCP/UDP spojení
10	Každé HW zařízení podporuje minimálně 18000 SSL transakcí za vteřinu pro RSA klíče s délkou 2048-bitů
11	Každé HW zařízení podporuje minimálně 9000 SSL transakcí za vteřinu pro klíče ECDSA s P-256
12	Vestavěná ochrana proti HTTP DoS útokům
13	Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10
14	Možnost doprogramovat si filtrovací pravidla pro aplikace
15	Ochrana AJAX a JSON aplikací
16	Detekce a ochrana před web scraping útoky
17	Detekce a ochrana před pokusy o prolomení logovacích stránek pomocí hrubé síly (brute force)
18	Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům)
19	Rozšířená podpora pro detekci aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu, detekce robotických klientů
20	Podpora odlišení lidských uživatelů od robotů pomocí Captcha
21	Zabezpečení XML komunikace
22	Podpora maskování/odstranění citlivých informací – např. rodné čísla, čísla kreditních karet apod.
23	Automatické nahrávání a aplikování nových signatur aplikačních útoků
24	Podpora pro vytváření vlastních signatur pro detekci HTTP útoků

25	Podpora pozitivního a negativního bezpečnostního modelu (pozitivní a negativní bezpečnostní logika)
26	Blokování útočníků na základě geolokace
27	Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP
28	Ochrana protokolů SMTP a FTP
29	Podpora SSL (šifrování a dešifrování)
30	Podpora ECDSA a podpora hybridních certifikátů (DSA/ECDSA/RSA)
31	Popdora symetrického šifrování včetně šifer Camellia
32	Podpora HTTP Strict Transport Security (HSTS)
33	Podpora HTTP/2
34	Podpora akcelerace
	- Konsolidace TCP spojení od klienta směrem k serveru tj. Z několika spojení od uživatele udělat jedno spojení na server
	- Caching
	- Komprese
	- Možnost optimalizace TCP stacku zvlášť směrem k uživateli a směrem k severu
35	Podpora různých typů reportů – PCI, geolokační reporty
36	Podpora standardů PCI DSS, HIPAA, Basel II a SOX
37	Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint aj.
38	Integrace s nástrojem na detekci zranitelností webových aplikací
39	Podpora pro monitoring a měření výkonu HTTP aplikací
40	Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů:
	· Cenzic Hailstorm
	· WhiteHat Sentinel
	· IBM Rational AppScan
	· QualysGuard Web Application Scanning
41	Podpora REST API pro správu zařízení
42	Autentikace klientů přes LDAP/Radius
43	Certifikace ICSA webového aplikačního firewallu
44	Možnost připojení k monitorovacím nástrojů třetích stran prostřednictvím otevřeného API
45	Možnost přidávat zákaznické požadavky na základě skriptovacího jazyka nebo obdobné technologie
46	Podpora Active-Active, Active-Passive módů
47	Granulární logování / logování per aplikace
48	K dispozici jako autonomní box nebo ve formě šasi
49	Management: sériový port, GUI, příkazový řádek, iLO
50	Podpora login a logout stránek pomocí AJAX/JSON
51	Mitigace DDoS útoků založená na behaviorální analýze
52	Povoleni jednotlivych HTTP metod pro jednotliva URL
53	Podpora více logovacích profilů pro danou aplikaci
54	Podpora WebSocketu
55	Prevence před únosy klientských HTTP relací „Session Hijacking"
56	Detekce anomalií sledovanim ID koncove stanice uzivatele
57	Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům)
58	Podpora virtualizace – separací IP adresního prostoru (obdoba VRF) nebo plnohodnotné virtualizace

59	Možnost rozšíření o funkci Web Aplikačního Firewalu dodatečnou licencí
60	Možnost rozšíření o funkci podpory externích šifrovacích karet (HSM) dodatečnou licencí

Technická specifikace funkcí ADC

Pol. č.	*Technické specifikace nabízeného řešení - Proxy server (ADC)*
1	2 ks HW zařízení s montáží do technologické 19" skříně (RACK), max. 2U
2	Plně redundantní napájecí zdroje AC
3	Nabízíme min. 6x 1Gbps optických Ethernet rozhraní nebo slotů a zároveň min. 4 x 10 Gbps optických rozhraní nebo slotů pro Ethernet
4	Nabízíme celkem 4x Ethernet moduly s podporou rychlosti 10 Gbps s vlnovou délkou 850 nm pro vlákno MMF (50/125)
5	Lights-out management - nezávislý servisní procesor pro vzálenou správu zařízení (vypnutí/zapnutí zařízení, konzolový přístup)
6	L4 propustnost každého HW zařízení minimálně 18 Gbps
7	L7 propustnost každého HW zařízení minimálně 18 Gbps
8	Každé HW zařízení podporuje minimálně 425 000 L4 spojení za sekundu
9	Každé HW zařízení podporje minimálně 20 milionů současných TCP/UDP spojení
10	Každé HW zařízení podporuje minimálně 18000 SSL transakcí za vteřinu pro RSA klíče s délkou 2048-bitů
11	Každé HW zařízení podporuje minimálně 9000 SSL transakcí za vteřinu pro klíče ECDSA s P-256
12	Podpora SSL certifikátů podepsaných SHA-2 metodou
13	Podpora TLS 1.2
15	Podpora AES-GCM a ECC pro TLS 1.2
16	Podpora STARTTLS pro SMTP provoz
17	Podpora šifrování pomocí Suite B, ECDSA, AES-GCM
18	Popdora symetrického šifrování včetně šifer Camellia
19	Podpora HTTP Strict Transport Security (HSTS)
20	Možnost pracovat až s 4096-bitovými klíči
21	Podpora hardwarové SSL akcelerace
22	Možnost zvýšit výkonnostní parametry SSL dokoupením licence
	Balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů až do 7. vrstvy OSI (ftp, dns, https/http, sip, ...)
	Klient/Server NAT/PAT
	Podpora různých typů rozkladu zátěže provozu:
	· Kruhová metoda s vážením
	· Podle počtu navázaných spojení
	· Podle otisku zdrojové a cílové adresy
	· Podle URL a cookie
23	· Na základě SNMP (např. zátěže procesorů)
24	· Podle vah pro skupiny
25	· Na základě počtu odezev od serverů
26	Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, L4 payloadu, HTTP cookie, HTTP obsahu, HTTP hlavičky, RADIUS atributů, RTSP hlavičky, SIP hlavičky, SSL Session ID
27	Podpora různých typů dostupnosti a zdraví aplikace (monitoring) - ICMP, DNS, HTTP, TCP/UDP port, SSL Hello, SMTP, RADIUS, LDAP, WMI...
28	Možnost kombinace více metod monitoringu (AND/OR)

29	Podpora modifikace HTTP provozu: · Vložení/přepsání cookie · Modifikace URL · Možnost vložit zdrojovou IP do L7 hlavičky · Modifikace HTTP obsahu
30	Podpora šablon pro konfiguraci balancingu aplikací – např. Microsoft Exchange Server 2010 a 2013 Client Access Servers,Citrix XenApp a XenDesktop
31	Možnost tyto šablony upravovat dle potřeb zákazníka
32	Podpora TCP multiplexingu
33	Podpora multipath TCP (MPTCP)
34	Podpora symetrické akcelerace Citrix ICA
35	Podpora ICAP protokolu
36	Podpora http komprese
37	Podpora http mezipaměti (cache)
38	Podpora filtrování paketů
39	Podpora QoS – markování, rate-limiting
40	Podpora TCP SYN cookie ochrany
41	Podpora SDN služeb – VXLAN virtualizace sítě
42	Podpora NVGRE a Transparent Ethernet Bridging tunelu
43	TDS/ MSSQL DB Proxy
44	Podpora Financial Information eXchange (FIX) protokolu
45	Podpora pro monitoring, manipulaci a modifikaci dat procházejícího datového provozu na základě skriptovacího jazyka nebo obdobné technologie
46	Podpora protokolu HTTP/2
47	Podpora IPv4/IPv6 brány
48	Plná podpora IPv6
49	Podpora 802.1Q
50	Podpora sFlow
51	Podpora IPFIX
52	Správa přes GUI, CLI
53	Podpora SNMP (1, 2c a 3)
54	Podpora SSH
55	Podpora vysokorychlostního logování pro každou aplikaci zvlášť
56	Podpora režimu redundance se synchronizací stavových tabulek (state failover)
57	Podpora redundantních clusterů Active-Standby i Active-Active
58	Možnost zapojit do redundantního clusteru různé typy HW nebo virtualizovaných platforem
59	Dostupnost jak hardwarového tak i virtuálního řešení
60	Podpora otevřeného API pro nástroje třetích stran pro konfiguraci a monitoring zařízení
61	Podpora virtualizace – separací IP adresního prostoru (obdoba VRF) nebo plnohodnotné virtualizace
62	Možnost rozšíření o funkci Web Aplikačního Firewalu dodatečnou licencí
63	Možnost rozšíření o funkci podpory externích šifrovacích karet (HSM) dodatečnou licencí

Specifikace implementačního procesu

První část - Specifikace implementačního procesu a nabízených produktů a výstupů řešení WAF

- Dodavatel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie webového aplikačního firewallu, jejíž obsah bude následující:
    - Popis terminologie, použité v dokumentu
    - Informace o stávajícím prostředí Zákazníka
    - Seznam aplikací, které budou WAF zabezpečeny
    - High-level popis řešení
    - Popis změny v infrastruktuře
    - High-level popis úpravy ovlivněných procesů např. řešení bezpečnostních incidentů
    - Řešení autentizace administrátorů WAF protokolem TACACS+
- Dodavatel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
    - Vymezení rozsahu řešení
    - Popis funkčních vlastností požadovaného zabezpečení aplikací technologií WAF
    - Popis úprav existujícího IT prostředí Zákazníka
    - Popis cílové úpravy vnitřních procesů
- Dodavatel vytvoří Low Level Design s následujícím obsahem:
    - Celkový návrh řešení
    - Typizované konfigurační šablony bezpečnostních politik WAF
    - Konfigurace WAF clusteru (zajištění konzistence bezpečnostních politik napříč clusterem WAF)
    - Konfigurace bezpečnostních politik
    - Ladění bezpečnostních politiky proti výskytu tzv. falešných poplachů
    - Konfigurace ochrany proti DoS a DDoS aplikačním útokům
    - Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace
    - Konfigurace spolupracujících systémů (MDM, Active Directory a další)
- Dodavatel připraví podrobné akceptační testy WAF
- Dodavatel provede pod dohledem Zákazníka akceptační testy WAF
- Dodavatel provede analýzu stávajících procesů zákazníka a připraví:
    - Soupis procesů, dotčených implementací WAF
    - Soupis rolí v rámci dotčených procesů
    - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
    - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
    - Přiřazení rolí k jednotlivým procesním krokům
- Dodavatel proškolí zástupce Zákazníka v:
    - Řešení a základní operativě
    - Upravených procesech
- Dodavatel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

- **Druhá část - Specifikace implementačního procesu a nabízených produktů a výstupů řešení ADC**
    - Dodavatel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie ADC, jejíž obsah bude následující:
        - Popis terminologie, použité v dokumentu
        - Informace o stávajícím prostředí Zákazníka

- Seznam aplikací, které budou ADC využívat
- High-level popis řešení
- Popis změny v infrastruktuře
- Řešení autentizace administrátorů ADC protokolem TACACS+

- Dodavatel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení rozsahu řešení
  - Popis funkčních vlastností požadovaného zabezpečení aplikací technologií ADC
  - Popis úprav existujícího IT prostředí Zákazníka
  - Popis cílové úpravy vnitřních procesů
- Dodavatel vytvoří Low Level Design s následujícím obsahem:
  - Celkový návrh řešení ADC
  - Typizované konfigurační šablony (soubor pravidel) pro řízení aplikačního provozu
  - Jmennou konvenci pro ADC řešení
  - Konfigurace ADC clusteru
  - Konfigurace politik řízení aplikačního provozu pro aplikace
  - Vytvoření a implementace standardů (soubor pravidel) pro SSL terminaci
  - Vytvoření a implementace standardů (soubor pravidel) pro monitoring aplikací
  - Vytvoření a implementace standardů (soubor pravidel) pro manipulaci s HTTP provozem (vkládání odebíraní HTTP záhlaví apod.)
  - Vytvoření a implementace standardů pro optimalizaci TCP a HTTP provozu
  - Konfigurace ochrany proti DoS a DDoS aplikačním útokům
  - Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace
  - Konfigurace spolupracujících systémů (MDM, Active Directory a další)
- Dodavatel ve spolupráci se Zákazníkem vytvoří plán scénářů vysoké dostupnosti aplikací
- Dodavatel připraví podrobné akceptační testy ADC
- Dodavatel provede pod dohledem Zákazníka akceptační testy ADC
- Dodavatel provede analýzu stávajících procesů zákazníka a připraví:
  - Soupis procesů, dotčených implementací ADC
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Dodavatel proškolí zástupce Zákazníka v:
  - Řešení a základní operativě
  - Upravených procesech
- Dodavatel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Katalogové č.	Popis	Počet kusů
Fáze 1	**Web aplikačního firewallu**	
F5-BIG-LTM-I4800	BIG-IP i4800 Local Traffic Manager (32 GB Memory, Max SSL, Max Compression)	2
F5-SVC-BIG-STD-L1-3	Level 1-3 Standard Service for BIG-IP (5x10)	10
F5-SVC-BIG-RMA-2	Next-Business-Day Hardware Replacement Service (RMA) for BIG-IP	10
F5-ADD-BIG-ASM-I4XXX	BIG-IP Application Security Manager Module for i4X00	2
F5-SVC-BIG-STD-L1-3	Level 1-3 Standard Service for BIG-IP (5x10)	10
F5-UPG-AC-I4XXX	BIG-IP Single AC Power Supply for i4X00 (250 W, Field Upgrade)	2
F5-UPG-SFP+-R	BIG-IP & VIPRION SFP+ 10GBASE-SR Transceiver (Short Range, 300 m, Field Upgrade)	4
SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	4

DRUHÁ ETAPA

Technická a implementační specifikace

Popis nabízeného řešení

Dodavatel nabízí dodávku dvojice zařízení webové proxy s centrálním managementem pro zajištění funkčních požadavků v oblasti webové bezpečnosti, který zajistí požadovanou službu a zvýší úroveň ochrany vnitřní sítě proti možným hrozbám obsaženým uvnitř webové komunikace.

Kontrola webové komunikace je poskytována zejména v těchto základních oblastech:

- Možnost filtrace prohlížení nevhodného obsahu
- Možnost ochrany proti komunikaci obsahující zavirovaný obsah
- Možnost ochrany proti komunikaci obsahující malware
- Možnost autentizace uživatelů komunikujících přes webovou proxy
- Možnost aplikační kontroly komunikující přes http a https protokol
- Možnost kontroly https protokolu (dekrypce HTTPS)
- Možnost omezení šířky pásma pro streamované aplikace
- Možnost centrálního monitoringu a reportingu webového provozu
- Možnost centrální správy a konfigurace politik
- Možnost nasazení webových proxy ve vysoké dostupnosti

Součástí dodávky budou i případné licence a to v počtu pro 700 uživatelů.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s aktuální verzí VKB.

- Řízení provozu
- Autentizace uživatelů a správců systému
- Logovaní
- Autorizace uživatelů a správců systému
- Použité šifrovací a hashovací algoritmy
- Vysoká dostupnost
- Atd.

Dále musí být provedena iniciální konfigurace a případná registrace licencí.

Technická specifikace nabízeného zařízení a SW

Nabízená specifikace na řešení webové proxy
Plně redundantní řešení
Řešení podporuje centralizovanou konfiguraci pomocí dedikované management appliance
Řešení podporuje balancování
Řešení poskytuje podporu na HW, licence a SW po dobu 5 let
Řešení je jednoduše škálovatelné pro případ rozšíření
Řešení může být výkonově dimenzováno na 1000 uživatelů a licencováno na 700 uživatelů

Jedno fyzické zařízení je schopné zpracovat minimálně 650 požadavků za sekundu při zapnutých všech bezpečnostních funkcích (NTLM ověřování uživatelů, HTTPS dešifrování, antivirus, antimalware, filtrování URL, proxy cache)
Malware kontrola a filtrování
Spyware/Adware/obecná ochrana proti webovým hrozbám
Antivirová ochrana
Automatická aktualizace všech antimalware signatur po 5 minutách nebo častěji
Podpora současného provozu více antimalware engines přímo na sobě (ne na dalším serveru)
AV engines
Ochrana proti phishing útokům
Automatická aktualizace pravidel na ochranu proti phishing útokům
Podpora filtrování URL
Minimálně 60 URL kategorií
Používané databáze pro URL/web filtrování
Vytváření politik per identita/uživatel
Definice politik dle časového okna
Definice politik dle URL kategorie
Definice politik pro cílové URL
Definice politik pro cílovou IP adresu
Možnost blokování
Možnost pouze monitorovat
Možnost zobrazit notifikační stránku při přístupu s možností potvrzení sdělení a vytvoření záznamu v logu
Možnost vytvoření vlastních URL kategorií
Kategorizace URL (domén) i vyšších řádů (subdomén)
Možnost filtrovat přístup na Webmail
Možnost filtrovat přístup na web chat aplikace
Dynamická kategorizace nekategorizovaných URL přímo na zařízení
Dynamická kategorizace nekategorizovaných URL v cloud výrobce
Filtrování na základě web reputace
Nastavitelné reputační filtrování na základě hodnoty reputace pro blokování/povolení/skenování obsahu
Blokování metody HTTP POST pomocí metadata (file type, file name, file size)
Plnohodnotné a pravdivé skenování obsahu pro detekci typu souboru
Skenování na vrstvě TCP pro detekci nakažených stanic s aplikacemi, které komunikují po nestandardních portech
Monitorování a blokování malware spojení na všech 65535 portech
Monitorování a blokování malware spojení v příchozím i odchozím směru
Proxy cache a výkon
Kapacita proxy cache minimálně 500 GB (v RAID)
Maximální velikost cacheovaného objektu alespoň 1 GB
Technologie proxy cache
Implementace v transparentním módu pomocí WCCPv2
Implementace v transparentním módu pomocí policy routingu nebo L4 přepínače
Implementace jako explicitní proxy
Implementace jako explicitní proxy pomocí PAC souboru anebo WPAD
Možnost hostování PAC souborů přímo na řešení

Podpora více upstream proxy s podmíněným směrováním HTTP provozu
Více datových portů pro skenování web provozu
Možnost současného provozu řešení v explicitním i transparentním módu
Kontrola protokolů pro kontrolu
HTTP
HTTPS (dešifrování provozu)
FTP over HTTP
FTP (native)
Filtrování dílčích elementů web stránek
Filtrování konkrétních typů prohlížečů a jejich verzí
Blokování Java
Blokování ActiveX
Detekované typy archivů
Detekce vnořených archivů
Blokování konkrétních typů souborů
Detekce a blokování šifrovaných souborů
Blokování souborů nad definovanou maximální velikost
Monitorování a blokování aplikací P2P, IM, Youtube, Facebook, Flash video na aplikační úrovni (AVC)
Možnost omezení šířky pásma pro media streaming provoz (youtube, atd...)
Granulární rozpoznávání obsahu stránek facebook (tzn. Povolení přístupu na facebook, ale blokování facebook chat, facebook video či facebook games)
Ověřování uživatelů
Autorizace uživatele na základě IP adresy
Autorizace uživatele na základě subnetu
Ověření uživatele oproti LDAP (LDAPS)
Active directory ověření uživatele pomocí NTLMSSP (integrované ověřování Windows) - NTLMv1, NTLMv2
Podpora LDAP/Active directory skupin pro přiřazení politik
Pro NTLM podpora Windows serverů 2000/2003/2008/2012
Podpora Kerberos
Administrace a management
HTTPS Management console
CLI přístup pomocí SSH
RS232 serial console port
Podpora centralizovaného managementu (vytváření konfigurace na jednom místě a poté její automatická distribuce)
Ověřování a autorizace administrátorů pomocí RADIUS
Ověřování administrátorů pomocí lokálních účtů
Neomezený počet vlastních (administrátorem definovaných) URL kategorií
Správa uživatelskými účty s různými právy
Napojení do centrálního dohledu pomocí SNMP
Podpora centrálního logování pomocí SYSLOG
Hardware a podpora (v případě realizace řešení více appliance se uvedené vlastnosti vztahují na každou z nich)

řešení má formu appliance s vlastním proprietárním operačním systémem
Podpora pro pět (5) GigabitEthernet rozhraní na hardware platformě
Více HDD v hardware RAID poli
Celková instalovaná disková kapacita minimálně 2,4 TB
32 GB RAM
CPU s multicore software podporou (alespoň 6 jader)
1U rack šasi
Poskytovaná podpora přímo od výrobce
Podpora výrobce formou email, telefon, web
Přístup na portál podpory výrobce a znalostní báze
Plná podpora hardware po dobu trvání kontraktu podpory
Reporting
GUI rozhraní pro účely administrace a prohlížení reportů
Možnost vlastního nastavení reportu
Možnost detailního prohlížení reportů pro každého uživatele a jeho aktivit pro účely analýzy
Export reportů a plánování jejich pravidelného zasílání
Zobrazení podezřelých aktivit pro každého uživatele
Top-N reporty pro: Top uživatele, top URL, top URL kategorie, top malware, používání web aplikací
Možnost ukládání reportu v PDF formátu

Specifikace nabízeného - centrální management
Řešení poskytuje podporu na HW, licence a SW po dobu 5 let
Řešení může být výkonově dimenzováno na 1000 web uživatelů. Licencováno na 700 web uživatelů
Jedno fyzické zařízení je schopné uchovat detailní data o každé transakci minimálně 3 měsíce zpětně bez použití externího uložiště při běžném provozu
Funkce Web Security Management a Reporting
Centralizovaná replikace konfigurace na více web security zařízení
Sdružování web security zařízení do skupin
Možnost delegace práv pro konfigurování pouze konkrétní politiky konkrétnímu administrátorovi
Správa web security zařízení s různými verzemi OS
Možnost skrýt nepřiřazené politiky pro delegovaného administrátora
Možnost zobrazit ostatní politiky pouze pro čtení pro delegovaného administrátora
Možnost plánování update politik na konkrétní čas
Centralizovaná kolekce dat od více web security zařízení
Vytváření konsolidovaných reportů z dat od více web security zařízení
Možnost sledování a dohledávání konkrétní transakce přes více web security zařízení pomocí jednoho GUI rozhraní
Vygenerování reportu on-demand o aktuální aktivitě daného uživatele
Historické ukládání reportů a dostupnosti reportovaných dat
Plánované reporty pro doručení
Administrace a management
HTTPS Management console
CLI přístup pomocí SSH

RS232 serial console port
Master administrator uživatel ověřován pomocí RADIUS/LDAP/MS AD
Administrátoři ověřováni pomocí lokálních účtů
Administrativní role pouze pro čtení
Možnost stateful backup všech web reportovaných dat na případném záložním management zařízení
Možnost plánování data backup
Hardware a podpora
Řešení má formu appliance s vlastním proprietárním operačním systémem
Zařízení je i formou virtuálního appliance do Vmware z důvodu redundance (rozšíření počtu virtuálních strojů musí být bezplatné)
Více HDD v hardware RAID poli v RAID 10
Celková instalovaná disková kapacita minimálně 3,6 TB
16 GB RAM
Alespoň 2x Hexa-core CPU s multicore software podporou
Maximálně 1U rack šasi
Poskytovaná podpora přímo od výrobce
Podpora výrobce formou email, telefon, web
Přístup na portál podpory výrobce a znalostní báze
Plná podpora hardware po dobu trvání kontraktu podpory

Specifikace implementačního procesu a nabízených produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie WEB proxy, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury WEB proxy a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, FW, AD, DHCP, DNS, CA, VPN gateway)
  - Identifikace tříd uživatelů a zařízení, specifikace přístupových politik
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis typu nasazení
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. PoC s následujícími kroky:
  - Instalace WEB proxy a zapojení do PoC infrastruktury
  - Integrace s potřebnou interní infrastrukturou (MS AD, CA, NTP, DNS, atd.)
  - Konfigurace a licencování
  - Nastavení politik dle funkční specifikace
  - Testování

- Zhotovitel připraví podrobné tzv. PoC akceptační testy
- Zhotovitel provede pod dohledem Objednatele PoC akceptační testy

Druhá část

- Zhotovitel vytvoří na základě úspěšně provedených akceptačních testů Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Typizované konfigurace jednotlivých typů přístupových politik
  - Konfigurace WEB proxy
  - Konfigurace spolupracujících systémů (FW, Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Třetí část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací WEB proxy
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Katalogové č.	Popis	Počet kusů
Fáze 2	**Webové proxy**	
WSA-S390-K9	WSA S390 WebSecurity Appliance with Software	2
CON-PSRT-S390	PRTNR SS 8X5XNBD WSA S390 WebSecurity	2
CCS-PWR-AC-770W	Cisco Content Sec AC Power Supply 770W for x90 appliance	4
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	4
SF-WSA-9.1.2-K9	WSA Async OS v9.1.2	2
CCS-HDD-BLNK	Content Sec 2.5 inch HDD blanking panel	8
CCS-MLOM-I-RJ45	Cisco Content Sec i350 MLOM NIC	2
CCS-CPU-E5-2620D	Content Sec 2.40 GHz E5-2620 v3/85W 6C/15MB Cache	2
CCS-MRAID-12G-1G	Cisco Content Sec 12Gbps SAS 1GB FBWC Cache module	2
CCS-MRAID-12G	Cisco Content Sec 12G SAS Modular Raid Controller	2
CCS-HDD-600GB	Content Sec 600GB 12G SAS 10K RPM SFF HDD (4K)	8
CCS-MEM-8GB-RV-A	Content Sec x90 8GB DDR4-2400-MHz RDIMM/PC4-19200	8
WSA-WSP-AMP-90D	Web Premium SW with AMP (WREP+WUC+AMAL+AMP) 90 Day License	2

WSA-WSP-AMP-90D-SW	Web Premium SW with AMP (WREP+WUC+AMAL+AMP) 90 Day License	2
WSA-L4TM-LIC	WSA L4 Traffic Monitoring License	2
WSA-CASM-LIC	WSA Cisco AnyConnect Secure Mobility License	2
WSA-HTTPS-LIC	WSA HTTPS Inspection License	2
WSA-PROXY-LIC	WSA Proxy and Dynamic Vectoring and Scanning License	2
WSA-WSP-LIC=	Web Premium SW Bundle (WREP+WUC+AMAL) Licenses	700
WSA-WSP-5Y-S3	Web Premium SW Bundle (WREP+WUC+AMAL) 5YR, 500-999 Users	700
SMA-M390-K9	SMA M390 Security Management Appliance with Software	1
CON-PSRT-SMA-M39K	PRTNR SS 8X5XNBD M390	1
CCS-PWR-AC-770W	Cisco Content Sec AC Power Supply 770W for x90 appliance	2
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
SF-SMA-10.1.0-K9	SMA Async OS v10.1.0	1
CCS-HDD-BLNK	Content Sec 2.5 inch HDD blanking panel	2
CCS-MEM-8GB-RV-A	Content Sec x90 8GB DDR4-2400-MHz RDIMM/PC4-19200	2
CCS-MRAID-12G	Cisco Content Sec 12G SAS Modular Raid Controller	1
CCS-MRAID-12G-1G	Cisco Content Sec 12Gbps SAS 1GB FBWC Cache module	1
CCS-HDD-600GB	Content Sec 600GB 12G SAS 10K RPM SFF HDD (4K)	6
CCS-CPU-E5-2620D	Content Sec 2.40 GHz E5-2620 v3/85W 6C/15MB Cache	2
CCS-MLOM-I-RJ45	Cisco Content Sec i350 MLOM NIC	1
SMA-WMG-90D	Web Management SW Bundle 90 Day License	1
SMA-WMG-90D-SW	Web Management SW Bundle 90 Day License	1
CCS-MESSAGING-LIC	Cisco Content Security Messaging License	1
SMA-WMGT-LIC=	SMA Centralized Web Management Reporting License	700
SMA-WMGT-5Y-S3	Web Management SW Bundle, 5YR License Key, 500-999 Users	700

TŘETÍ ETAPA

Technická a implementační specifikace

Popis nabízeného řešení

Dodavatel nabízí dodávku dvojice zařízení Next-Generation Firewall v redundantním režimu active-standby pro zajištění vysoké dostupnosti. NGFW bude zajišťovat segmentaci sítě, pokročilou analýzu provozu a filtrovaní provozu ve vnitřní síti OLK.

NGFW poskytuje funkcionalitu zejména v těchto základních oblastech:

- Oddělení sítí dle typu připojených zařízení – segmentace sítě a ochrana jednotlivých segmentů
- Filtrování provozu dle požadovaných komunikací
- Pokročilé inspekce protokolů (až do L7 ISO OSI)
- Prevence a detekce útoků na úrovni síťového provozu
- Ochrana proti Malware hrozbám s dynamickou analýzou (sandboxing)
- Možnost podpory URL filtrace
- Možnost využívání znalostní databáze výrobce pro blokaci nebezpečných zdrojů (nebezpečné IP adresy, URL nebo DNS domény v Internetu)
- Možnost centrálního managementu společného pro oba NGFW
- Možnost centralizovaného nastavení bezpečnostních politik
- Možnost centralizované distribuce nových verzí sw a aktualizací
- Management musí poskytovat správu a řízení uživatelů, jejich oprávnění a monitoring
- Zajištění podpory výrobce při řešení funkčních problémů

Součástí dodávky jsou i případné licence.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s platným a účinným zákonem o kybernetické bezepečnosti.

- Řízení provozu
- Autentizace uživatelů a správců systému
- Logování
- Autorizace uživatelů a správců systému
- Použité šifrovací a hashovací algoritmy
- Vysoká dostupnost
- Atd.

Dále je i řešena iniciální konfigurace a registrace licencí NGFW.

Technická specifikace zařízení a SW

Dodané zařízení splňuje všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti

Výkon a funkcionalita firewallu	
Formát zařízení	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	8
Možnost rozšíření o moduly rozhraní	2
Možnost rozšíření o další 10Gb SFP+ rozhraní	8
Možnost rozšíření o další 40Gb SFP+ rozhraní	4
Redundantní zdroje	-
Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.10M/4.5M
Rychlost vytváření nových spojení přes stavový FW	Min. 150K/s
Propustnost stavového firewallu (multiprotokolový režim)	Min. 10 Gbps
Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 12 Gbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	Min. 10 Gbps
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 4 Gbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 2.5 Gbps
VPN propustnost	Min. 8 Gbps
Současný počet VPN spojení (IPSec/SSL)	Min. 10.000
Podpora L2 (transparentního) módu s podporou NAT a PAT	-
Podpora L3 (routovaného) módu s podporou NAT a PAT	-
Podporovaný počet VLAN	Min. 1024
Podpora stateful failover	active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	-
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	-
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	-
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	-
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů	-
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	-
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	-
Podpora Policy based Routing	-
Podpora kontroly paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	-
Podpora filtrace IPv4, IPv6	-
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	-
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	-
Podpora inspekce IPv6 provozu	-
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	-
Podpora NAT64 a DNS64	-
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	-
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	-

Možnost rozšíření o funkce NextGen FW	-
Možnost rozšíření o funkce NextGen IPS	-
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	-
Zohlednění kontextových informací o koncovém zařízení (typ, stav, apod.) a využití ve filtrech	-
API rozhraní pro sdílení kontextových informací s dalšími systémy	-
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	-
Funkce IPS a anti-malware	
Možnost definovat typ provozu předávaný k inspekci do IPS	-
Podpora také IDS režimu – pasivního monitorování (TAP režim)	-
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	-
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	-
Podpora 802.1Q tagovaných rámců	-
Podpora různých IPS politik pro různé typy provozu	-
Inspekce pro IPv4 i IPv6	-
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	-
IPS obsahuje filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	-
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	-
Podpora aplikace pro psaní zákaznických filtrů	-
Podpora importu komunitních filtrů/signatur Snort	-
IPS umí detekovat a blokovat útoky průzkumných aktivit	-
IPS podporuje adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	-
IPS umí detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host" jako je spyware, phishing nebo Botnet C&C	-
IPS umí detekovat a blokovat útoky proti síťové infrastruktuře Objednatele, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále poskytuje i ochranu pro protokoly využívané v IP telefonii	-
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	-
Možnost vyhledávání typu signatury v centrální databázi výrobců podle typu a závažnosti útoku	-
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	-
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	-
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	-
Možnost definice uživatelské vrstvy politik	-
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	-
Různé politiky lze sdílet a aplikovat na různé senzory	-
Podpora aktivní online ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV výrobců	-
Ochrana před malware typu „zero day attack" které nelze detekovat tradičními antiviry	-
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	-
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	-

Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	-
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru výrobce jako malware je na koncových stanicích okamžitě přesunut do karantény	-
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	-
IPS je možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	-
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation"	-
Možnost automatické i manuální klasifikace stanice jako "kritické" se zohledněním v pravidlech, reportech apod.	-
Podpora „remediation" modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	-
Otevřené rozhraní pro uživatelsky vytvářené „remediation" moduly	-
Podpora databází reputací adres v Internetu (Security Intelligence)	-
Funkce Next-Gen FW	
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	-
Podpora pasivního monitorování (TAP režim)	-
Podpora 802.1Q tagovaných rámců	-
Podporovaných aplikací	Min. 3000
Kategorie aplikací (nebezpečné, důležité, apod.)	-
Filtrace podle typů aplikací webových i ne-webových	-
Filtrace podle reputace serverů	-
SSL inspekce (dekrypce/enkrypce)	-
Security Inteligence database – známé uzly botnet sítí C&C	-
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	-
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	-
Možnost integrovat vlastní reputační databáze	-
Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)	-
Filtry mohou zohlednit roli a identitu uživatele	-
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	-
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	-
Řešení je schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti
Přehled o síťových spojeních má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování

	Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact" aplikace Množství přenesených dat
Správa	
Vzdálená správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	-
Přístup ke GUI http/https protokolem	-
Možnost vzdáleného přístupem protokolem ssh přímo do FW	-
Možnost přístupu k textovým logům (syslog) přímo ve FW	-
Možnost centrální správy při nasazení více firewallů	-
Při centrální správě: možnost sdílených bezpečnostních politik	-
Při použití clusteru se spravuje pouze jeden logický prvek	-
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	-
Zobrazení logů a událostí v grafickém rozhraní správy	-
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	-
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	-
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	-
Centrální dohledová konzole je schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	-
Centrální dohledová konzole je schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	-
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	-
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	-
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	-
Pro reporty lze definovat template definující formát a obsah reportu	-
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	-

V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	-
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	-
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	-
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	-
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	-
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	-
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	-
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	-
Podpora řízeného přístupu podle rolí administrátorů	-
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	-
Možnost založit pro daný incident „ticket" přímo v prostředí GUI managementu	-
Workflow pro předávání „ticketů" mezi administrátory	-
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu" pro další analýzu	-
Možnost definice politik pro sledování odpovídajících parametrů „zdraví" na senzorech a centralizované konzoli (zatížení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	-
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví"	-
Různé politiky pro sledování „zdraví" lze aplikovat na různé senzory nebo centralizovanou konzoli	-

Specifikace implementačního procesu a požadovaných produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie NGFW, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury NGFW a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, AD, DHCP, DNS, CA, atd.)
  - Identifikace tříd uživatelů a zařízení, specifikace komunikační matice
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis implementovaných funkcí
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel vytvoří Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Konfigurace NGFW
  - Požadavky pro konfigurace spolupracujících systémů (Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Druhá část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací NGFW
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Katalogové č.	Popis	Počet kusů
Fáze 3	**Next Generation IPS/Firewallu**	
FPR4110-BUN	Cisco Firepower 4110 Master Bundle	1
FPR4110-NGFW-K9	Cisco Firepower 4110 NGFW Appliance, 1U, 2 x NetMod Bays	2
CON-PSRT-FPR4110N	PRTNR SS 8X5XNBD Cisco Firepower 4110	2
CAB-AC-EUR	Power Cord - Europe, 16/10A,250V, 2500mm, -40C to +85C	2
SF-F4K-FXOS-2.3-K9	Cisco FXOS v2.3 for FPR4100	2
SF-F4K-TD6.2.3-K9	Cisco Firepower Threat Defense software v6.2.3 for FPR4100	2
FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	2
FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	2
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	2
FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit	2
FPR4K-FAN	Firepower 4000 Series Fan	12
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	2
FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	2
FPR4K-PSU-BLANK	Firepower 4000 Series Chassis Power Supply Blank Slot Cover	2
FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	2
FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	2
L-FPR4110T-TMC=	Cisco FPR4110 Threat Defense Threat, Malware and URL License	2
L-FPR4110T-TMC-5Y	Cisco FPR4110 Threat Defense Threat, Malware and URL 5Y Subs	2
SF-FMC-VMW-2-K9	Cisco Firepower Management Center, (VMWare) for 2 devices	1
CON-PSBU-SFMMCVWK	PSS SWSS UPGRADES Cisco Firepower Management Center, (VMWa	1

ČTVRTÁ ETAPA

Technická a implementační specifikace

High-level popis nabízeného řešení

Stávající stav

Síť KÚOK je vybavena na přístupové vrstvě přepínači Cisco, řady Catalyst 2960 (WS-C2960X-48TD-L) a C4510R. WiFi síť je postavená na bázi Cisco WLC AIR-CT2504 a AP řad CAP702, AP1131, CAP1552EU a CAP1602. Jako VPN koncentrátor slouží firewall ASA 5585.

Počty zařízení a klientů jsou následující:

Typ zařízení	Počet aktuálně	Počet s výhledem
AP	8	14
WLC	1	2
Přepínače	26	30
IP telefon	10	10
Tiskárny	70	85
Ostatní pasivní zařízení	17	30
Pracovní stanice	536	600
Notebook	203	250
Zařízení externistů/dodavatelů	70	90
Mobilní telefony	236	270

Tablety	79	100
VPN gateway	2	2

Základem autentizace a autorizace v síti je doména s 2 řadiči Active Directory. Tyto uzly současně realizují certifikační autoritu. Certifikační autorita vydává certifikáty stanicím pro přihlášení do interní WiFi. Záplaty jsou na stanice distribuovány pomocí WSUS serverů a SW je instalován a vzdálená podpora je poskytována z Microsoft SCCM serveru. DHCP služby jsou poskytovány z dedikovaného serveru.

V rámci jiného výběrového řízení bude implementován systém MDM, který bude spravovat mobilní zařízení interních uživatelů.

Nabízené řešení

Dodavatel nabízí dodání redundantního autentizačního systému pro autentizaci zařízení a uživatelů v LAN a WiFi prostřednictvím protokolu 802.1X a zařízení a uživatelů, přistupujících vzdáleně do sítě Objednatele prostřednictvím VPN. Přístup bude sjednocen na stejnou úroveň oprávnění ve všech třech přístupových technologiích. Mimo interních a externích uživatelů bude autentizační systém ověřovat i Guest uživatele pomocí stávajícího portálu na bezdrátovém kontroléru a musí disponovat vlastnostmi pro onboarding privátních i firemních mobilních zařízení.

Autentizační systém bude ověřovat i přístup administrátorů na síťové prvky protokolem RADIUS a TACACS+, včetně autorizace oprávnění administrátorů na jednotlivých prvcích.

Mezi očekávané přínosy patří:

1. zabezpečení přístupu s možností karantény zařízení, která neodpovídají politice
2. zjednodušení konfigurace přepínačů
3. podpora mobility uživatelů
4. snadnější segmentace podle rolí uživatelů a snadnější vynucení přístupových oprávnění na prvcích, chránících datacentrum.

Autentizační systém je schopen nativního začlenění do existující MS domény, ve které bude ověřovat interní uživatele protokolem Kerberos a ze které bude získávat podklady pro autorizaci uživatelů a zařízení. Autentizace doménových stanic a uživatelů musí být zajištěna takovým mechanismem, že se v jednom kroku ověří jak stanice, tak i uživatelé, obojí protokolem 802.1X. Pouze v případě, že se úspěšně ověří jak stanice, tak i uživatel, bude povolen přístup do sítě. Rámcové požadavky na autentizaci jsou uvedeny v tabulce níže. Systém je schopen zajistit bezproblémový provoz uživatelské autentizace na bázi uživatelského jména a hesla současně s uživatelskými certifikáty.

Autentizační systém je schopen ověřit zdraví Windows pracovních stanic a podle výsledku autorizovat stanici do karantény nebo do produkční VLAN. Karanténa musí být realizovatelná jako karanténní VLAN nebo přístup omezený pomocí ACL. Autentizační systém je současně schopen spolupracovat se systémy MDM a SCCM v rámci autorizačních rozhodnutí. Z obou systémů musí být schopen získat informaci o stavu zařízení, resp. jeho shodě s požadovanou politikou. Zdraví stanic musí být periodicky ověřovatelné a v případě, že stanice nebude v souladu s požadavky, musí systém umožnit uvedení stanice do souladu pomocí „wizardu", který uživatele procesem povede.

Rámcová autentizační matice pro LAN a WiFi

Uživatel/zařízení	Interní uživatel	Externí uživatel s účtem v doméně	Externí uživatel bez účtu v doméně (servisní technik)	Guest	Autentizace zařízení
Doménová stanice	ověření stanice+ověření uživatele (U/P+CERT) Posture/SCCM kontrola	ověření stanice+ověření uživatele (U/P+CERT) Posture/SCCM kontrola	x	x	certifikát zařízení
Doménový notebook	ověření stanice+ověření uživatele (U/P+CERT) Posture/SCCM kontrola	ověření stanice+ověření uživatele (U/P+C Posture/SCCM kontrola ERT)	x	x	certifikát zařízení
Pracovní stanice mimo doménu	x	x	MAC adresa	Guest portál a U/P	
Zařízení bez 802.1X suplikanta	x	x	x	x	MAC adresa
Mobilní zařízení pod MDM	jen autentizace zařízení	jen autentizace zařízení	x	x	certifikát zařízení ověření v MDM
Mobilní zařízení mimo MDM	x	x	x	Guest portál a U/P	x

Rámcová autentizační matice pro VPN

Uživatel/zařízení	Interní uživatel	Externí uživatel s účtem v doméně	Externí uživatel bez účtu v doméně (servisní technik)
Doménový notebook	ověření uživatele (U/P+CERT) Posture/SCCM kontrola	x	x
Pracovní stanice mimo doménu	x	ověření uživatele (U/P+CERT) Posture kontrola	x
Mobilní zařízení pod MDM	ověření uživatele (U/P+CERT)	x	x
Mobilní zařízení mimo MDM	x	x	x

Autentizační systém je, samostatně nebo ve spojení s jiným integrovaným SW systémem, schopen nabídnout následující vlastnosti pro začlenění do stávajících technických procesů:

1. autorizace operací založená na rolích
2. autorizace registrace MAC adres do skupin založená na rolích

3. disponuje připravenými workflow pro registraci MAC adres pro pasivní zařízení, externisty, pro případ selhání 802.1X autentizace na stanicích, re-image, blacklisting a další
4. umožňuje full-text prohledávání databáze MAC adres
5. automatická expirace registrované MAC adresy ke stanovenému času a jejich automatické mazání z databáze autentizačního systému
6. prezentace aktuálních i historických autentizačních relací, jejich stavu a detailu autentizačních relací z autentizačního systému
7. možnost náhledu na atributy uživatelských účtů v Active Directory
8. možnost náhledu na konfiguraci portů přepínačů
9. možnost náhledu na stav autentizace z pohledu přepínačů
10. možnost black-listingu zařízení s jejich okamžitým odpojením od sítě

Autentizační systém nebo jeho doplňková SW komponenta je schopna zabezpečit WoL v prostředí se změnou VLAN mezi autentizací stanice a uživatele.

Systém je výkonnostně dimenzován pro autentizaci zhruba 2000 koncových zařízení (včetně uživatelských stanic, mobilních zařízení a Guest uživatelů) a administrátorů na cca. 50 síťových zařízení.

Zhotovitel zajistí potřebné licence v odpovídajícím počtu.

Technická specifikace zařízení a SW

Požadovaná funkcionalita/vlastnost
Obecná charakteristika ověřovacího řešení
Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.)
Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1X) a pro VPN přístup
Poskytuje AAA funkce (viz níže)
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)
Je dostupné ve formě Virtuálního stroje na platformách Vmware, Linux KVM a Microsoft Hyper-V
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)
Podporované protokoly
RADIUS pro autentizaci, autorizaci, zaznamenávání
Proxy funkce pro externí RADIUS
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST
Podpora TACACS+ pro centrální řízení administrativního přístupu na síťová zařízení
Podporované databáze uživatelů (s možností definovat pořadí průchodu)
Interní (pro uživatele i koncová zařízení)
Podpora více nezávislých Active Directory
LDAP (RFC 2251)
RADIUS Token indentity source (RFC 2865)
RSA RADIUS token server
Certifikační profil
Ověřování uživatelů a zařízení
Ověření uživatelů/zařízení heslem nebo certifikátem

Ověření MAC adresou připojovaného zařízení
Autorizace: pružný systém pro definici pravidel pro přístup k síti
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:
uživatele (role, skupiny)
stavu a typu koncového zařízení (viz níže)
místa připojení
historie připojení
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě
Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu"
Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti
Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)
Accounting
Zaznamenávání aktivity uživatelů a zařízení připojených k síti
Dotazovací systém, korelace záznamů, centralizované výkazy
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)
Funkce GUEST serveru
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi
Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů
Samoobslužný portál pro uživatele
Ověření přes HTTP a HTTPS
Propojení se SMS bránou pro zasílání Guest účtu
Propojení s email serverem pro zasílání Guest účtu
Rozpoznávání typu koncových zařízení
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)
Předdefinované profily pro síťová zařízení NAD od různých vendorů
Podpora pro IPv6 koncová zařízení
Podpora BYOD
Onboarding (registrace, provisioning, nastavení klientských zařízení)
Onboarding/provisioning proces formou samoobsluhy
Specifické politiky pro BYOD zařízení
Možnost nastavení limitu BYOD zařízení pro jednoho uživatele
Interní CA, pro vydávání certifikátů BYOD zařízením
Interní CA lze řetězit jako subordinate pod firemní CA
Podpora MDM
Workflow pro registrace do MDM
Výměna informací z MDM platformy a využití v politikách (např. pokud zařízení je „compliant")
Ovládání MDM přímo z prostředků bezpečnostního managementu (zamykání, mazání, apod.) zařízení
Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení)
Rozpoznávání stavu koncových zařízení a jeho náprava
Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat:

instalovaný operační systém
opravy instalované v operačním systému
hodnoty položek v registry databázi systémů Windows
stav aplikací, zejména antivirů, antispyware, antimalware a firewall
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)
Varianta agentů s GUI i bez GUI
Další vlastnosti
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)
Podpora SXP (Exchange Protocol) dle IETF
Otevřené API pro podporu propojení se zařízeními třetích stran
Distribuce identitních informací na další bezpečnostní síťové prvky, které ji budou využívat pro zajištění jejich vlastní funkčnosti (webová proxy, NGIPS, ...)
Podpora komunikace s Microsoft SCCM pro zjištění stavu zařízení z pohledu SW záplat a instalovaného SW.
Rozhraní nebo externí aplikace pro centralizovanou správu MAC adres a provozní troubleshooting s následujícími vlastnostmi
Autorizace operací založená na rolích, definovaných v AD
Autorizace registrace MAC adres do skupin založená na rolích, definovaných v AD
Disponuje připravenými workflow pro registraci MAC adres pro pasivní zařízení externisty, pro případ selhání 802.1X autentizace na stanicích, re-image, blacklisting a další
Umožňuje full-text prohledávání databáze MAC adres a auditování provedených operací
Registrace MAC adres a automatická expirace registrované MAC adresy ke stanovenému času a jejich automatické mazání z databáze
Prezentace aktuálních i historických autentizačních sessions, jejich stavu a detailu autentizační session
Možnost náhledu na atributy uživatelských účtů v Active Directory
Možnost náhledu na konfiguraci portů přepínačů
Možnost náhledu na stav autentizace z pohledu přepínačů
Umožňuje operace provádět prostřednictvím REST API
Funkce pro správu ověřovacího systému
Centralizovaná správa
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému
Zjednodušení správy vytvářením skupin uživatelů, koncových a síťových zařízení
Grafické rozhraní pro definici pravidel přístupu k síti
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)
Zaznamenávání událostí na externí syslog server
Podpora SNMPv3
NTP pro synchronizaci času
SMTP pro zasílání zpráv a výstrah přes e-mail

Specifikace implementačního procesu a požadovaných produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie 802.1X, autentizace administrátorů na síťové prvky a autentizace do VPN, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury přístupových technologií, zahrnutých do řešení a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, VPN, AD, DHCP, DNS, CA, VPN gateway)
  - Identifikace tříd uživatelů a zařízení, specifikace autentizačních scénářů

- High-level popis řešení
- Potřebné změny v infrastruktuře
- High-level popis úpravy ovlivněných procesů
- Řešení autentizace administrátorů na síťové prvky protokolem TACACS+

- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis autentizačních scénářů
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. PoC s následujícími kroky:
  - Instalace Cisco ISE a zapojení do PoC infrastruktury
  - Integrace s Cisco WLC nastavení politik dle funkční specifikace
  - Konfigurace WLC pro 802.1X a definované scénáře
  - Nastavení Cisco ISE
  - Integrace Cisco ISE s MDM
  - Konfigurace autentizačních, autorizačních, profilačních a posture politik
  - Konfigurace a otestování nativních suplikantů a Anyconnect klienta
  - Vytvoření zadání pro instalaci a konfiguraci aplikací pro centrální správu MAC adres a pro provozní troubleshooting 802.1X řešení,
  - Instalace a konfigurace aplikací pro centrální správu MAC adres a pro provozní troubleshooting 802.1X řešení,
  - Testování autentizačních scénářů
  - Konfigurace Guest řešení
  - Konfigurace VPN řešení
  - Konfigurace vzorových síťových prvků pro autentizaci, autorizaci a accounting přístupu administrátorů
- Zhotovitel připraví podrobné tzv. PoC akceptační testy
- Zhotovitel provede pod dohledem Objednatele PoC akceptační testy

Druhá část

- Zhotovitel vytvoří na základě úspěšně provedených akceptačních testů Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Typizované konfigurace jednotlivých typů síťových prvků
  - Konfigurace Cisco ISE
  - Konfigurace suplikantů
  - Konfigurace aplikací pro centrální správu MAC adres a pro provozní troubleshooting
  - Konfigurace spolupracujících systémů (MDM, Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Třetí část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:

- Soupis procesů, dotčených implementací 802.1X, autentizace administrátorů a přístupu do VPN
- Soupis rolí v rámci dotčených procesů
- Návrh úpravy procesů tak, aby byly po implementaci systému funkční
- Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
- Přiřazení rolí k jednotlivým procesním krokům

- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Katalogové č.	Popis	Počet kusů
Fáze 4	**Systém pro řízení přístupu do komunikační infrastruktury**	
L-ISE-BSE-PLIC	Cisco ISE Base License	1
L-ISE-BSE-P4	Cisco ISE Base License - Sessions 1000 to 2499	2000
L-ISE-PLS-LIC=	Cisco ISE Plus License	100
L-ISE-PLS-5Y-S1	Cisco ISE Plus License, 5Y, 100 - 249 Sessions	100
L-ISE-APX-LIC=	Cisco ISE Apex License	1500
L-ISE-APX-5Y-S4	Cisco ISE Apex License, 5Y, 1000 - 2499 Sessions	1500
L-ISE-TACACS-ND=	Cisco ISE Device Admin Node License	2
SNS-3515-K9	Small Secure Network Server for ISE Applications	2
CON-PSRT-SNS3515K	PRTNR SS 8X5XNBD Small Secure Network Server for ISE Appl	2
SW-3515-ISE-K9	Cisco ISE Software for the SNS-3515-K9 appliance	2
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
SNS-HD600G10K12G	600GB SAS 10K RPM HDD	2
SNS-MRAID12G-1GB	1GB FBWC for Cisco 12G SAS Modular RAID	2
SNS-PSU1-770W	770W power supply	2
R2XX-RAID0	Enable RAID 0 Setting	2
SNS-CPU-E52620D	2.40 GHz E5-2620 v3/6C	2
SNS-MLOM-IRJ45	MLOM Intel -Quad Port 1Gb RJ45	2
SNS-MR-1X081RV-A	8GB DDR4-2400	4
SNS-MRAID12G	Avila Cisco 12G SAS Modular Raid Controller	2
	Podpůrné aplikace	
APL-MAB-BASE-1Y	AleFIT MAB Keeper Base License - 1year	5
APL-MAB-DEVICE-1Y-1000	AleFIT MAB Keeper Device license - 1year - 1000devices	10
APL-OL-BASE-1Y	AleFIT Office locator Base License - 1year	5
APL-OL-DEVICE-1Y-1000	AleFIT Office Locator Device license - 1year - 1000devices	10
PÁTÁ ETAPA		

Technická a implementační specifikace

Popis nabízeného řešení

Dodavatel nabízí dodávku zařízení (HW nebo virtuální appliance) pro zajištění funkčních požadavků v oblasti Enterprise Mobility Managementu - EMM, který zajistí požadovanou službu a podporu automatizace nastavení mobilních zařízení, distribuce firemních mobilních aplikací, certifikátů, konfigurací a profilů.

Řízení mobilních zařízení je nutné zejména v těchto základních oblastech:

- řízení a správa povolených přístupů do vnitřní sítě
- centralizované nastavení bezpečnostních politik
- zajištění bezpečnosti firemních dat, dokumentů a přístupu k nim (aktualizace, vynucení politik, blokace, výmaz dat)
- centralizace dohledu připojených mobilních zařízení do sítě
- řízená distribuce mobilních aplikací
- centralizovaná distribuce bezpečnostních certifikátů
- podpora instalace, aktualizace a nastavení zařízení a aplikací
- správa a řízení uživatelů, oprávnění, restrikce, monitoring
- možná podpora uživatele při problémech se zařízením/aplikací

Součástí dodávky jsou i případné licence a to v počtu pro 200 mobilních zařízení.

Součásti dodávky je implementace řešení a to takovým způsobem, aby zde byl soulad s platným a účinným zákonem o kybernetické bezpečnosti.

- Řízení provozu
- Autentizace uživatelů a správců systému
- Logovaní
- Autorizace uživatelů a správců systému
- Použité šifrovací a hashovací algoritmy
- Vysoká dostupnost
- Atd.

Dále musí být řešena iniciální konfigurace (autokonfigurace) a registrace připojeného mobilního zařízení. Řešení musí umožňovat kromě registrace nového mobilního zařízení administrátorem i možnost registrace nového mobilního zařízení samotným uživatelem a automatické přiřazení bezpečnostních politik.

Technická specifikace zařízení a SW

Funkční požadavky
Automaticky omezuje přístup k EMM na počet mobilních zařízení vázaných na jednoho zaměstnance/uživatele.
EMM kompatibilita. • Vyžadováno mobilní OS: Android, iOS, Windows 10
Zhotovitel zajistí pravidelné aktualizace EMM o podporu aktualizovaných OS a nových typů mobilních zařízení dle aktuálních trendů na trhu mobilních zařízení.
EMM Bezpečnost
Centralizované a vynucené nastavení bezpečnostních politik na mobilních zařízeních před tím než je na zařízení možno přistupovat k firemním aplikacím a datům a do firemní sítě.
Možnost validace OS mobilního zařízení a jeho kompatibilita s vyžadovanými bezpečnostními politikami.
Možnost vyhodnotit mobilní zařízení, kde bylo manipulováno s OS zařízení (jailbrake devices, rooted devices).
Možnost vynucení PIN/PASSWORD na mobilním zařízení.
Možnost vynucení automatického zamykání při neaktivitě.
Podpora uživatelské autorizace přes interní certifikáty.
Možnost white list / black list mobilního zařízení.
Interoperabilita s wifi infrastrukturou pro řízení přístupu mobilních zařízení do wifi sítě pro:

• On-boarding ... automatizovaný proces nastavení zařízení pro přístup do sítě – generování/distribuce certifikátu. • Profiling ... nastavení bezpečnostních profilů a oprávnění přístupů do sítě. • Posture ... ověření stavu, zdali zařízení smí být připojeno do příslušné sítě.
Možnost vytvoření dedikované oblasti pro firemní aplikace a data se zabezpečením (zabezpečený kontejner). Pro oddělení soukromých a privátních dat, tzv. vytvoření samostatné zabezpečené oblasti na mobilním zařízení pro uložení firemních mobilních aplikací, firemních dat a certifikátů. Možnost zabránit kopírovat data mimo dedikovaný kontejner pro firemní data.
Podpora technologií Samsung Knox a Android for Work.
Možnost online blokovat přístup mobilnímu zařízení k firemním zdrojům (email, file share, atd.) v případě nesplnění bezpečnostních požadavků na mobilní zařízení.
Podpora vzdáleného smazání mobilního zařízení, které je řízeno bezpečnostní politikou z EMM.
Možnost napojení na centralizovaný dohled. Možnost odesílání logů do externího systému (SIEM/syslog sever).
EMM SW Inventory
Možnost nastavit automatickou distribuci firemních mobilních aplikací na cílové mobilní zařízení pomocí jednotlivých profilů řízených v EMM. Zajištění Centralizované správy firemních aplikací a přístupů na mobilním zařízení.
Možnost vzdálené obnovy aplikační vrstvy na cílovém zařízení z centrálního úložiště firemních mobilních aplikací.
Podpora centralizované správy mobilního zařízení za použití interní evidence (IMEI, SIM) s vazbou na profil mobilních zařízení řízených pomocí EMM.
Podpora pro řízenou distribuci aktualizací firemních mobilních aplikací, certifikátů a oprávnění na mobilní zařízení podle profilu.
Součástí EMM je vlastní Store pro uložení firemních mobilních aplikací. Možnost omezit dostupnost aplikací pro instalaci na firemní mobilní zařízení v rámci oficiálních application store – Google Play, Apple Store, Microsoft.
EMM podpora SSO a interních autorizačních credentials poskytovaných Microsoft AD.
Podpora selective wipe, tedy možnost vzdáleného smazání centrálně distribuovaných aplikací z EMM.
Možnost vytváření whitelist a blacklist seznamů pro mobilní aplikace a následné využití těchto seznamů v bezpečnostních politikách pro řízení přístupu mobilních zařízení k firemním prostředkům.

Požadované možnosti nasazení EMM

On-Premise:

- HW appliance
- Virtuální appliance s podporou VMWare a Hyper-V

Specifikace implementačního procesu a nabízených produktů a výstupů

První část

- Zhotovitel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie EMM, správa mobilních zařízení a řízení přístupu mobilních zařízení k firemním prostředkům a datům, jejíž obsah bude následující:
  - Popis terminologie použité v dokumentu
  - Informace o stávajícím prostředí Objednatele
  - Popis architektury EMM a všech IT systémů, které mají vztah k implementaci (LAN, WiFi, FW, AD, DHCP, DNS, CA, VPN gateway)
  - Identifikace tříd uživatelů a zařízení, specifikace registračních scénářů
  - High-level popis řešení
  - Potřebné změny v infrastruktuře
  - High-level popis úpravy ovlivněných procesů
  - Řešení autentizace administrátorů
- Zhotovitel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  - Vymezení scope řešení
  - Popis funkčních vlastností požadovaného řešení
  - Popis úprav existujícího IT prostředí Objednatele
  - Popis registračních scénářů
  - Popis profilů pro jednotlivé mobilní OS
  - Popis cílové úpravy vnitřních procesů
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. PoC s následujícími kroky:
  - Instalace EMM a zapojení do PoC infrastruktury
  - Integrace s potřebnou interní infrastrukturou (MS AD, CA, NTP, DNS, atd.)
  - Nastavení politik dle funkční specifikace
  - Konfigurace, registrace a otestování vybraných mobilních zařízení
  - Vytvoření zadání pro instalaci a konfiguraci aplikací pod centrální správou
  - Instalace a konfigurace aplikací pod centrální správou EMM
  - Testování scénářů přístupu pomocí mobilních zařízení
- Zhotovitel připraví podrobné tzv. PoC akceptační testy
- Zhotovitel provede pod dohledem Objednatele PoC akceptační testy

Druhá část

- Zhotovitel vytvoří na základě úspěšně provedených akceptačních testů Low Level Design s následujícím obsahem:
  - Celkový návrh řešení
  - Typizované konfigurace jednotlivých typů využívaných mobilních OS
  - Konfigurace EMM
  - Registrace mobilních zařízení
  - Konfigurace aplikací pod centrální správou
  - Konfigurace spolupracujících systémů (FW, Active Directory a další)
- Zhotovitel připraví ve spolupráci s Objednatelem tzv. Pilotní implementaci v omezeném produkčním prostředí, nakonfiguruje ve spolupráci s Objednatelem jednotlivé komponenty produkčního prostředí, bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení (spolupráce Objednatele spočívá v přípravě stávajících systémů na spojení)
- Zhotovitel připraví podrobné tzv. Pilotní akceptační testy
- Zhotovitel provede pod dohledem Objednatele Pilotní akceptační testy

Třetí část

- Zhotovitel provede analýzu stávajících procesů Objednatele a připraví:
  - Soupis procesů, dotčených implementací EMM
  - Soupis rolí v rámci dotčených procesů
  - Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  - Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  - Přiřazení rolí k jednotlivým procesním krokům
- Zhotovitel proškolí zástupce Objednatele v:
  - Řešení a základní operativě
  - Upravených procesech
- Zhotovitel provede implementaci řešení v produkčním prostředí a bude spolupracovat na řešení vzniklých provozních problémů a případně upraví implementované řešení
- Zhotovitel připraví detailní tzv. Implementační testy
- Zhotovitel provede pod dohledem Objednatele Implementační testy
- Zhotovitel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

Katalogové č.	Popis	Počet kusů
Fáze 5	**Mobile Device Management systému**	
MI-EMG-D-PL	EMM Gold Perpetual License Per Device On Premise	200
MI-EMG-D-1YM-A	EMM Gold Perpetual Assurance Support Per Device On Premise Upgraded 5Y	200

Příloha č. 8 Smlouvy

Položkový rozpočet

Část Díla*	Počet jednotek**	Cena za jednotku v Kč bez DPH zobrazená na 2 desetinná místa	Cena za jednotku v Kč včetně DPH zaokrouhlená na 2 desetinná místa	Cena celkem v Kč bez DPH zaokrouhlená na 2 desetinná místa	Cena celkem v Kč včetně DPH zaokrouhlená na 2 desetinná místa
Implementace Web aplikačního firewallu					
BIG-IP i4800 Local Traffic Manager (32 GB Memory, Max SSL, Max Compression)	2	887 195,81 Kč	1 073 506,93 Kč	1 774 391,62 Kč	2 147 013,86 Kč
Level 1-3 Standard Service for BIG-IP (5x10)	10	127 120,59 Kč	153 815,92 Kč	1 271 205,94 Kč	1 538 159,18 Kč
Next-Business-Day Hardware Replacement Service (RMA) for BIG-IP	10	21 186,77 Kč	25 635,99 Kč	211 867,66 Kč	256 359,86 Kč
BIG-IP Application Security Manager Module for i4X00	2	485 799,81 Kč	587 817,78 Kč	971 599,63 Kč	1 175 635,55 Kč
Level 1-3 Standard Service for BIG-IP (5x10)	10	69 607,14 Kč	84 224,64 Kč	696 071,38 Kč	842 246,36 Kč
BIG-IP Single AC Power Supply for i4X00 (250 W, Field Upgrade)	2	36 980,74 Kč	44 746,70 Kč	73 961,49 Kč	89 493,40 Kč
BIG-IP & VIPRION SFP+ 10GBASE-SR Transceiver (Short Range, 300 m, Field Upgrade)	4	33 801,77 Kč	40 900,14 Kč	135 207,07 Kč	163 600,56 Kč
10GBASE-SR SFP Module, Enterprise-Class	4	7 567,56 Kč	9 156,75 Kč	30 270,24 Kč	36 626,99 Kč
Instalace a implementace	1	700 000,00 Kč	847 000,00 Kč	700 000,00 Kč	847 000,00 Kč
Celkem				5 864 575,02 Kč	7 096 135,77 Kč
Implementace Webové proxy					
WSA S390 WebSecurity Appliance with Software	2	164 989,44 Kč	199 637,22 Kč	329 978,88 Kč	399 274,44 Kč
PRTNR SS 8X5XNBD WSA S390 WebSecurity	2	62 924,58 Kč	76 138,75 Kč	125 849,17 Kč	152 277,50 Kč
Web Premium SW Bundle (WREP+WUC+AMAL) 5YR, 500-999 Users	700	2 260,07 Kč	2 734,68 Kč	1 582 046,93 Kč	1 914 276,78 Kč
PRTNR SS 8X5XNBD M390	1	71 955,21 Kč	87 065,80 Kč	71 955,21 Kč	87 065,80 Kč
SMA M390 Security Management Appliance with Software	1	182 748,72 Kč	221 125,95 Kč	182 748,72 Kč	221 125,95 Kč
Web Management SW Bundle, 5YR License Key, 500-999 Users	700	201,88 Kč	244,28 Kč	141 318,04 Kč	170 994,83 Kč
Instalace a implementace	1	800 000,00 Kč	968 000,00 Kč	800 000,00 Kč	968 000,00 Kč

Celkem				3 233 896,94 Kč	3 913 015,30 Kč
Implementace Next Generation IPS/Firewallu					
Cisco Firepower 4110 NGFW Appliance, 1U, 2 x NetMod Bays	2	934 458,58 Kč	1 130 694,89 Kč	1 868 917,17 Kč	2 261 389,77 Kč
PRTNR SS 8X5XNBD Cisco Firepower 4110	2	473 509,99 Kč	572 947,09 Kč	947 019,98 Kč	1 145 894,18 Kč
Cisco FPR4110 Threat Defense Threat, Malware and URL 5Y Subs	2	1 993 951,81 Kč	2 412 681,69 Kč	3 987 903,61 Kč	4 825 363,37 Kč
Cisco Firepower Management Center, (VMWare) for 2 devices	1	5 012,70 Kč	6 065,37 Kč	5 012,70 Kč	6 065,37 Kč
PSS SWSS UPGRADES Cisco Firepower Management Center, (VMWa	1	6 577,47 Kč	7 958,74 Kč	6 577,47 Kč	7 958,74 Kč
Instalace a implementace	1	500 000,00 Kč	605 000,00 Kč	500 000,00 Kč	605 000,00 Kč
Celkem				7 315 430,93 Kč	8 851 671,43 Kč
Implementace systému pro řízení přístupu do komunikační infrastruktury úřadu					
Cisco ISE Base License - Sessions 1000 to 2499	2000	130,35 Kč	157,73 Kč	260 706,60 Kč	315 454,99 Kč
Cisco ISE Plus License, 5Y, 100 - 249 Sessions	100	592,99 Kč	717,52 Kč	59 299,32 Kč	71 752,17 Kč
Cisco ISE Apex License, 5Y, 1000 - 2499 Sessions	1500	420,56 Kč	508,88 Kč	630 841,37 Kč	763 318,05 Kč
Cisco ISE Device Admin Node License	2	228 690,00 Kč	276 714,90 Kč	457 380,00 Kč	553 429,80 Kč
PRTNR SS 8X5XNBD Small Secure Network Server for ISE Appl	2	256 069,74 Kč	309 844,38 Kč	512 139,47 Kč	619 688,76 Kč
Cisco ISE Software for the SNS-3515-K9 appliance	2	343 513,17 Kč	415 650,94 Kč	687 026,34 Kč	831 301,87 Kč
AleFIT MAB Keeper Base License - 1year	5	131 670,00 Kč	159 320,70 Kč	658 350,00 Kč	796 603,50 Kč
AleFIT MAB Keeper Device license - 1year - 1000devices	10	24 255,00 Kč	29 348,55 Kč	242 550,00 Kč	293 485,50 Kč
AleFIT Office locator Base License - 1year	5	90 090,00 Kč	109 008,90 Kč	450 450,00 Kč	545 044,50 Kč
AleFIT Office Locator Device license - 1year - 1000devices	10	17 325,00 Kč	20 963,25 Kč	173 250,00 Kč	209 632,50 Kč
Instalace a implementace	1	900 000,00 Kč	1 089 000,00 Kč	900 000,00 Kč	1 089 000,00 Kč
Celkem				5 031 993,10 Kč	6 088 711,65 Kč
Implementace Mobile Device Management systému					
EMM Gold Perpetual License Per Device On Premise	200	2 290,32 Kč	2 771,29 Kč	458 064,02 Kč	554 257,46 Kč
EMM Gold Perpetual Assurance Support Per Device On Premise Upgraded 5Y	200	2 159,85 Kč	2 613,42 Kč	431 970,00 Kč	522 683,70 Kč
Instalace a implementace	1	300 000,00 Kč	363 000,00 Kč	300 000,00 Kč	363 000,00 Kč
Celkem				1 190 034,02 Kč	1 439 941,16 Kč
Penetrační testy					
Penetrační testy	1 soubor	450 000,00 Kč	544 500,00 Kč	450 000,00 Kč	544 500,00 Kč

Celkem				450 000,00 Kč	544 500,00 Kč
Publicita projektu					
Informační billboard	1 ks	50 000,00 Kč	60 500,00 Kč	50 000,00 Kč	60 500,00 Kč
Pamětní deska	1 ks	10 000,00 Kč	12 100,00 Kč	10 000,00 Kč	12 100,00 Kč
Celkem				60 000,00 Kč	72 600,00 Kč
Cena za Dílo				23 145 930,00 Kč	28 006 575,30 Kč

Servis	**Cena za měsíc v Kč bez DPH zobrazená na 2 desetinná místa**	**Cena za měsíc v Kč včetně DPH zaokrouhlená na 2 desetinná místa**	**Cena za 48 měsíců v Kč bez DPH zaokrouhlená na 2 desetinná místa**	**Cena za 48 měsíců v Kč včetně DPH zaokrouhlená na 2 desetinná místa**
Poskytování Servisních služeb	45 000,00 Kč	54 450,00 Kč	2 160 000,00 Kč	2 613 600,00 Kč

Nabídková cena v Kč bez DPH	
Cena za Dílo	**23 145 930,00 Kč**
Cena za 48 měsíců poskytování Servisních služeb	**2 160 000,00 Kč**
Celkem	**25 305 930,00 Kč**

Příloha č. 9 Smlouvy

Harmonogram

Pokyn pro účastníka: *Účastník doplní termíny dokončení příslušných částí etap Díla. Termíny budou stanoveny v celých kalendářních dnech s pevně stanoveným počátkem, kterým může nabytí účinnosti Smlouvy, ukončení jiné etapy, nebo ukončení jiné části etapy. Např. termín úspěšného dokončení druhé části První etapy může být stanoven takto: „do 20 kalendářních dnů ode dne dokončení první části První etapy". Etapy Díla lze provádět nezávisle na sobě i paralelně, nikoliv dle předpokládaného pořadí. Tj. např. pátá etapa může předcházet třetí etapě, druhá a čtvrtá etapa mohou být prováděny současně apod. Účastník je v povinen dodržet lhůtu pro provedení Díla dle odst. 39 této Smlouvy.*

etapa Díla	část etapy Díla	termín úspěšného dokončení části etapy Díla
První etapa	první část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	druhá část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
Druhá etapa	první část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	druhá část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	třetí část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
Třetí etapa	první část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	druhá část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
Čtvrtá etapa	první část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	druhá část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	třetí část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
Pátá etapa	první část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	druhá část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy
	třetí část	do 150 kalendářních dnů od nabytí účinnosti Smlouvy

[redacted]

Příloha č. 10 Smlouvy

Poddodavatelé

Seznam poddodavatelů

Dodavatel **MERIT GROUP a.s.**, IČO: 64609995, se sídlem: Březinova 136/7, Olomouc, PSČ 779 00 (dále jen ***„dodavatel"***), ako účastník zadávacího řízení veřejné zakázky s názvem Kybernetická bezpečnost Krajského úřadu Olomouckého kraje II, tímto v souladu s § 105 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, čestně prohlašuje, že mu nejsou známi poddodavatelé, jež se budou podílet na plnění veřejné zakázky.

V Olomouci, dne 7. 5. 2019
MERIT GROUP a.s.
Petr Weigel, statutární ředitel

[redacted]

.....
(podpis)