Smlouva o dílo

(číslo u Objednatele: 2025/0444/PÚ)
(číslo u Zhotovitele: 000 489/ 2025)

uzavřená podle § 2586 a násl.
zákona č. 89/2012 Sb., občanský zákoník
(dále jen „smlouva")

I. Smluvní strany

Objednatel: **Město Kyjov**
se sídlem Masarykovo náměstí 30/1, 697 01 Kyjov
IČ: 00285030
DIČ: CZ00285030
Jednající Mgr. Františkem Luklem, MPA, starostou města
Bankovní spojení: Komerční banka, a.s., číslo účtu: 1887430267/0100

Zhotovitel: **AXENTA a.s.**
se sídlem Mlýnská 326/13, 602 00 Brno
zapsaná v Obchodním rejstříku vedeném u KS v Brně, oddíl B, vložka 5888
IČ: 28349822
DIČ: CZ283498225
Jednající Ing. Lukášem Přibylem, předsedou představenstva
Bankovní spojení: Raiffeisenbank a.s., číslo účtu: 4291128001/5500

II. Předmět smlouvy

1. Tato Smlouva je uzavírána v rámci veřejné zakázky s názvem „Dodávka firewallu a log managementu“.
2. Zhotovitel bere na vědomí, že veřejná zakázka je spolufinancována v rámci Integrovaného regionálního operačního programu z prostředků Evropské unie a státního rozpočtu České republiky, název projektu: „Rozvoj elektronických služeb města Kyjov“, registrační číslo projektu: CZ.06.01.01/00/22_009/0002604.
3. Předmětem smlouvy je dodávka NGFW a Log managementu s 5letou podporou v souladu se specifikací dle přílohy 1 a 2 této smlouvy.
4. Objednatel se zavazuje za podmínek stanovených v této smlouvě dílo převzít a za jeho provedení zaplatit cenu, jejíž výše a způsob úhrady jsou uvedeny v článku VII. této smlouvy.

III. Součinnost Objednatele

1. Objednatel se zavazuje poskytnout Zhotoviteli k zajištění předmětu této smlouvy potřebnou součinnost.
2. Smluvní strany se dohodly, že Objednatel poskytne Zhotoviteli k provedení díla potřebné informace, přístup k technickým prostředkům pro potřeby implementace a dále časový prostor techniků Objednatele.

IV. Způsob plnění díla

1. Zhotovitel a Objednatel se dohodli, že předmět plnění smlouvy bude předán v celku po dokončení díla. O jeho předání bude sepsán písemný předávací protokol.
2. Zhotovitel provede dílo v souladu s platnými právními předpisy samostatně a při provádění díla je vázán pouze pokyny Objednatele.
3. Servisní podpora k produktům bude poskytována po dobu 5 let od účinnosti smlouvy v souladu se zadávacími podmínkami veřejné zakázky.
4. Místem plnění je sídlo Objednatele.
5. Zhotovitel je povinen provádět dílo v souladu se zájmy objednatele, řádně a s náležitou odbornou péčí. Zhotovitel je povinen provádět dílo tak, aby svou činností nebo prohlášením při plnění díla neohrozil či neporušil pověst, dobré jméno nebo důvěryhodnost objednatele.

VI. Dodací lhůta a místo plnění

1. Předpokládané zahájení plnění veřejné zakázky: ihned po nabytí účinnosti smlouvy
2. Termín dodání a implementace: do 2 kalendářních měsíců od nabytí účinnosti smlouvy. Termín dodání je závazný v tom případě, budou-li součinnosti Objednatele uvedené v bodě IV. této smlouvy probíhat bez zbytečného prodlení.
3. Servisní podpora k produktům bude poskytována po dobu 5 let od termínu předání díla (po implementaci) a to dle podmínek specifikovaných v příloze č. 4.
4. Místo plnění veřejné zakázky: Kyjov, Masarykovo náměstí 30/1

VII. Cena díla, platební podmínky a způsob fakturace

1. Cena je uvedena v příloze č. 3 Smlouvy, která je nedílnou součástí smlouvy.
2. Právo Zhotovitele vystavit fakturu za dodávku a implementaci firewallu a log managementu bez servisní podpory, tj. na částku 420.596,80 Kč bez DPH vzniká předáním díla a podpisem předávacího protokolu Objednatelem.

3. Právo Zhotovitele vystavit fakturu za poskytování servisní podpory k produktům ve výši 1/5 z celkové ceny servisní podpory uvedené v příloze č. 3 Smlouvy, tj. 192.968,16 Kč bez DPH vzniká vždy před započetím každého jednoho roku poskytování servisní podpory.
4. Objednatel je povinen zaplatit Zhotoviteli bezhotovostně cenu stanovenou podle odst. 1. tohoto článku na základě faktury vystavené Zhotovitelem.
5. Podkladem pro zaplacení je faktura, která bude splňovat všechny náležitosti daňového dokladu (pro plátce DPH), účetního dokladu a musí obsahovat číslo smlouvy Objednatele. Faktura, která bude zahrnovat dodávku a implementaci firewallu a log managementu bez servisní podpory bude obsahovat také text: „Spolufinancováno v rámci Integrovaného regionálního operačního programu z projektu: „Rozvoj elektronických služeb města Kyjov", registrační číslo projektu: CZ.06.01.01/00/22_009/0002604. Přílohou faktury musí být doklad o předání a převzetí plnění (Předávací protokol) podepsaný oprávněnými osobami obou smluvních stran. Zhotovitel je povinen vystavit fakturu nejpozději do patnácti (15) kalendářních dnů ode dne data uskutečnění zdanitelného plnění, kterým je den podpisu Předávacího protokolu.
6. Splatnost faktury je čtrnáct (14) kalendářních dnů ode dne, kdy byla Objednateli doručena.
7. Oprávněnou osobou k podpisu předávacího protokolu za stranu Zhotovitele je Ing. Lukáš Přibyl.
8. Oprávněnou osobou k podpisu předávacího protokolu za stranu Objednatele je Tomáš Pantlík, informatik.

VIII. Důvěrnost informací a nakládání s osobními údaji

1. Zhotovitel se zavazuje zachovat mlčenlivost o všech informacích, jež se při plnění předmětu smlouvy nebo v souvislosti s tímto plněním dozví (ústně, písemně, prostřednictvím prostředků elektronických komunikací nebo jakýmkoliv jiným způsobem, případně prostřednictvím jakéhokoliv nosiče informací) a:

    a) které Objednatel označí jako tajné či důvěrné, nebo

    b) o nichž je podle příslušných právních předpisů povinen mlčenlivost zachovávat též Objednatel, resp. členové jeho orgánů, zaměstnanci či osoby činné pro Objednatele, nebo

    c) o nichž se Zhotovitel může důvodně domnívat, že Objednatel bude mít zájem na jejich utajení nebo že jejich utajení je v zájmu Objednatele;

tato povinnost neplatí pro případy, kdy je zpřístupnění určitých informací vyžadováno právními předpisy.

2. Zhotovitel je povinen k této mlčenlivosti a ochraně obchodního tajemství zavázat i osoby, které případně použije při realizaci předmětu smlouvy.

IX. Záruka za dílo

1. Zhotovitel se zavazuje, že předmět díla bude bez vad a nedodělků, bude splňovat veškeré požadavky stanovené obecně závaznými právními předpisy a dílo bude způsobilé pro použití ke smluvenému, jinak k obvyklému účelu a že si dílo zachová smluvené, jinak obvyklé vlastnosti. Zhotovitel poskytuje záruku na implementaci řešení o délce 24 měsíců. Záruka se nevztahuje na dodaný SW, kde se tato část řeší v licenčních podmínkách výrobce.

2. Vzniklé vady po písemném uplatnění reklamace odstraní zhotovitel na svůj náklad, a to ve lhůtě stanovené objednatelem. Pokud objednatel nestanoví jinou lhůtu, zhotovitel je povinen odstranit vzniklé vady do 30 kalendářních dnů od jejich písemného uplatnění. Vady znemožňující výkon předmětu podnikání objednatele odstraní zhotovitel neprodleně.

X. Odpovědnost – smluvní pokuty

1. Zhotovitel odpovídá objednateli za škodu způsobenou objednateli v důsledku porušení povinností zhotovitele vyplývajících z této smlouvy a z obecně závazných právních předpisů.
2. Zhotovitel se zavazuje zaplatit objednateli smluvní pokutu ve výši 0,05 % z ceny díla za každý i započatý den prodlení zhotovení díla nebo odstranění vady vč. dílčích termínů plnění.
3. Zhotovitel se zavazuje zaplatit objednateli smluvní pokutu ve výši 0,05 % z roční částky za poskytování servisní podpory k produktům za každý započatý den prodlení s poskytováním servisní podpory, případně neposkytnutí servisní podpory v dohodnutém termínu.
4. Smluvní pokuty dle tohoto článku jsou splatné ve lhůtě 30 dnů od doručení výzvy k zaplacení smluvní pokuty.
5. Pro případ nedodržení termínu splatnosti sjednávají smluvní strany úrok z prodlení, jehož roční výše odpovídá nařízení vlády č. 351/2013 Sb., ve znění pozdějších předpisů.
6. Ustanovení o smluvní pokutě nemá vliv na právo objednatele požadovat náhradu vzniklé škody.

XI. Zvláštní ujednání

1. Smluvní strany se dohodly, že doručování písemností Objednateli bude směrováno na adresu Objednatele uvedenou v této smlouvě. Není-li možno adresátu písemnost doručit, považuje se písemnost za doručenou prvním dnem po uplynutí úložní lhůty, i když se adresát o uložení nedozvěděl.

2. V pochybnostech, nebo není-li prokázán jiný den doručení, se veškeré písemnosti doručované v souvislosti s touto smlouvou považují za doručené nejpozději 3. den ode dne podání písemnosti k poštovní přepravě formou doporučené zásilky. V případě doručování e-mailem se za okamžik doručení považuje okamžik, kdy adresát potvrdí přijetí e-mailu odesílateli, nejpozději však 10:00 následujícího pracovního dne. Při doručování prostřednictvím datové schránky se za okamžik doručení považuje přihlášení smluvní strany do datové schránky, do níž byla datová zpráva doručena, nejpozději však 10:00 následujícího pracovního dne.

XII. Závěrečná ustanovení

1. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění této smlouvy v registru smluv postupem podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.
2. Zhotovitel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (Centra pro regionální rozvoj ČR, MMR, MF, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen

vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

3. Zhotovitel je povinen uchovávat veškerou dokumentaci související s realizací projektu, z kterého je veřejná zakázka spolufinancována, včetně účetních dokladů minimálně do 31. 12. 2035. Pokud je v českých právních předpisech stanovena lhůta delší, musí být použita pro úschovu delší lhůta.
4. Zhotovitel je osobou povinnou spolupůsobit při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů. Zhotovitel bere na vědomí a souhlasí, že kontrola podle tohoto odstavce smlouvy může být provedena i v jeho sídle či pobočce. Pro účely kontroly se zhotovitel zavazuje uchovávat veškerou dokumentaci související s plněním předmětu smlouvy
5. V otázkách, které nebyly touto smlouvou specifikovány, se smluvní strany řídí obecně závaznými právními předpisy.
6. Smlouvu lze měnit jen dohodou smluvních stran, písemnými oboustranně podepsanými dodatky.
7. Dojde-li k odstoupení od smlouvy, hradí odstupující strana náklady spojené s realizací smlouvy straně druhé v prokázané výši.
8. Tato smlouva je vyhotovena ve dvou exemplářích, z nichž jedno vyhotovení obdrží Objednatel a jedno vyhotovení obdrží Zhotovitel.
9. Smluvní strany jsou si vědomy, že tato smlouva bude zveřejněna v Registru smluv v souladu se zákonem č. 340/2015 Sb., o registru smluv a zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, a to nejpozději do 30 dnů ode dne uzavření této smlouvy. Pokud je smluvní stranou subjekt povinný zveřejnit tuto smlouvu v Registru smluv, smluvní strany se dohodly, že tuto smlouvu do Registru smluv vloží Objednatel. Za zveřejnění této smlouvy si nebudou smluvní strany nic platit ani nahrazovat či poskytovat. Smluvní strany souhlasně prohlašují, že platnost tohoto ujednání zůstává zachována i v případě zániku nebo neplatnosti této smlouvy.
10. O uzavření této smlouvy rozhodla Rada města Kyjova na své 75. schůzi dne 9. 6. 2025.
11. Nedílnou součástí Smlouvy tvoří tyto přílohy:

Příloha č. 1: Firewall včetně vzdáleného přístupu

Příloha č. 2: Nástroj pro záznam a vyhodnocení logových událostí (Log Management)

Příloha č. 3: Cenový rozpočet

Příloha č. 4: Náležitosti poskytování servisních zásahů

V Kyjově dne dle el. podpisu
Za Objednatele

Mgr. František Lukl MPA
Digitálně podepsal Mgr. František Lukl MPA
Datum: 2025.07.09 13:02:01 +02'00'

.....

Mgr. František Lukl, MPA, starosta města

V Brně dne dle el. podpisu
Za Zhotovitele

Ing. Lukáš Přibyl
Digitálně podepsal Ing. Lukáš Přibyl
Datum: 2025.07.08 17:26:14 +02'00'

.....

Ing. Lukáš Přibyl, předseda představenstva

Příloha č. 1: Firewall včetně vzdáleného přístupu

FIREWALL VČETNĚ VZDÁLENÉHO PŘÍSTUPU (VPN)

ŘEŠENÍ OCHRANY PERIMETRU POČÍTAČOVÉ SÍTĚ

Současná ochrana perimetru poč. sítě neodpovídá aktuálním požadavkům na síťovou bezpečnost a klade neúměrné nároky na údržbu a správu. S ohledem na důležitost zařízení, výpadek této služby má vliv na chod celé instituce.

Z tohoto důvodu je poptáván hardwarový box. Oproti stávajícímu řešení, požadujeme služby antivirové kontroly provozu, antispam, application control, web filtering a intrusion prevention systém s možností aktualizací reputačních či jiných databází po dobu 5-ti let. Systém také musí využívat databázi IP reputation pro blokaci DoS útoků. Firewal musí taktéž obsahovat funkce web aplikačního firewalu pro ochranu webových aplikací, předpokládá se základní ochrana pomocí statických signatur. Redundantní konektivita se zbytkem síťové infrastruktury je samozřejmostí. Next Generation Firewall (dále jen NGFW) ve formě hardware appliance, s podporou výrobce v režimu 24x7 a aktualizací všech požadovaných bezpečnostních funkcí po dobu 5-ti let, musí také zabezpečit šifrovaný vzdálený přístup (VPN) do lokální poč. sítě.

Zadavatel si vyhrazuje právo otestování shody udávaných parametrů propustnosti jednotlivých bezpečnostních funkcí s reálným měřením/chováním zařízení v testovacím prostředí. S ohledem na požadavky zadávací dokumentace mohou být/budou testovány zejména tyto funkce:

- test kapacity firewallu (UDP PPS test, test propustnosti UDP/64B),
- test počtu konkurenčních spojení (TCP),
- test počtu nově navazovaných spojení,
- test propustnosti NGFW,
- možnosti správy, logování a reporting.

SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

NGFW - 1 kusy

Obecné minimální požadavky na NGFW

- hardware appliance o velikosti 1 RU
- podpora režimu vysoké dostupnosti (active/passive, active/active)
- správa zařízení pracujících v režimu vysoké dostupnosti musí probíhat prostřednictvím jednoho konfiguračního rozhraní, je požadována automatická synchronizace provozních a stavových informací mezi jednotlivými zařízení v jednom celku vysoké dostupnosti
- grafické konfigurační rozhraní a příkazový řádek
- minimální počty požadovaných síťových rozhraní:
  - 16x GE RJ 45
  - 4x 10 GE SFP+
  - management rozhraní 1x RJ 45
  - konzole sériové linky pro přístup k příkazovému řádku
- Podpora plnohodnotné inspekce síťového provozu v režimech
  - NAT/router
  - L2 transparentní režim (dva a více síťových rozhraní)

Minimální výkonové požadavky

Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání.

- minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 27 Gbps (udp pakety o velikosti 512 B)
- nízké vložené zpoždění zařízení (latence)
- minimální počet současně navázaných spojení firewallu 3M
- minimální počet nových spojení za sekundu 100 k
- propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)
  - propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) min. 3,1 Gbps
  - propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 2,8 Gbps
  - propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 5 Gbps

- propustnost funkce SSL inspekce provozu min. 3 Gbps
- min. počet konfigurovatelných virtuálních kontextů na každém zařízení 10

Funkční požadavky

- Podpora a zabezpečení IT systémů minimálně s ohledem na tyto bezpečnostní funkce:
  - funkce rozpoznávání aplikací na L7 – aplikační vrstvě, podpora alespoň 4000 aplikací, protokolů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací
  - funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů
  - ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT); předání zkoumaných souborů pro analýzu v prostředí typu sandbox
  - funkce kategorizace webových stránek (web filtering) s podporou minimálně 300 mil. známých URL (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze.
  - funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky z SSL inspekce požadujeme minimálně:
    - na základě administrátorem definovaných adres
    - na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví, atd.)
- ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius)
- funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky
- funkce QoS, traffic shaping
- funkce klientské VPN (přístup do vpn v tunelovém režimu s vpn klientem; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů; ssl vpn nebo ipsec vpn)
- site-to-site ipsec vpn s podporou statického i dynamického routování
- **ochrana proti SQL Injection a obecným útokům**
- **detekce a blokování** známých útoků na webové aplikace pomocí signatur a omezení

Součástí dodávky je instalace a konfigurace včetně připojení do počítačové sítě příslušnými moduly a kabely.

Vlastnosti zařízení

Požadovaná funkcionalita	Specifikace minimálních požadavků	Dodavatelem nabízená hodnota
Firewal mód	Routed/Transparent	Routed/Transparent
Podpora HA active/standby, active/active	ANO	ANO
Minimální počet 1Gb RJ-45 portů	16	16
Minimální počet 10Gb SFP+ portů	4	8
Min. 1x integrovaný management port	1Gb RJ-45	1Gb RJ-45
Min. 1x sériový port	RJ-45 console	RJ-45 console
Racková montáž	ANO	ANO
Podpora rozdělení na více virtuálních jednotek	ANO	10
Intrusion Prevention System	ANO	ANO
Visibilita aplikací	ANO	ANO
Detekce malware, sandboxing	ANO	ANO
Podpora SSL/TLS dešifrace	ANO	ANO
URL filtering	ANO	ANO
Remote access VPN (SSL VPN i IPSec)	ANO	ANO
Podpora Site-to-Site VPN	ANO	ANO
Podpora IPv4, IPv6	ANO	ANO
Min. VLAN subinterfaces	ANO	4095
Podpora EtherChannel 802.3ad	ANO	ANO

Příloha č. 2: Nástroj pro záznam a vyhodnocení logových událostí (Log Management)

Zadání

V rámci zvýšení kybernetické bezpečnosti bude začleněna technologie Log Managementu jako specializovaného bezpečnostního řešení, které umožňuje sbírat, parsovat, optimalizovat a analyzovat události ze všech možných vrstev IT infrastruktury.

LM řešení bude nedílnou součástí monitoringu kybernetické bezpečnosti města. Řešení Log Management, v rámci projektu, je uvažováno s konfigurovatelným uživatelským oddělením rolí s využitím silných šifrovacích metod a ochranou logů před neoprávněným přístupem k citlivým datům.

V rámci implementace požadujeme napojení všech relevantních zdrojů, jejich rozsah bude upřesněn v rámci návrhu cílového konceptu nasazení Log Managementu.

Požadujeme dodání cloudového řešení, kdy na straně města bude potřebný kolektor pro sběr logů a samotné uložení, zpracování a uchování logů bude na straně vendora případně dodavatele. Požadujeme přímý přístup k logovým záznamů minimálně v rozsahu potřebném pro jejich vyhodnocení. Dále požadujeme od dodatele servis v rozsahu nutném pro zajištění bezchybné funkce LM a sběru dat. Případně změny nebo napojení dalších zdrojů nepožadujeme zahrnout do nabídky, ale bude řešeno ve formě poptávky a nabídky ze strany zadavatele. Pro transparentnost požadujeme do nabídky uvést cenu za hodni práce servisního technika.

Ze strany dodavatele také požadujeme zajištění servisního rozhraní ve formě helpdesku pro zadávání servisních požadavků.

Obecné vlastnosti

Log Management bude řešením, které bude seskupovat provozní a bezpečnostní záznamy z HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity.

Požadujeme přehledné webovému rozhraní pro vyhledávání v logových záznamech, přizpůsobitelné reporty a statistiky, tak aby Log Management umožnil snazší práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

Požadované řešení bude nyní sloužit primárně jako Log Management, ale požadujeme dodání řešeni, které bude rozšiřitelné o část SIEM (v rámci řešení, nebo jako další součást) s tím, že nyní bude technicky využita pouze část Log Managementu.

Požadované funkční a nefunkční vlastnosti Log Managementu

Požadujeme řešení, které umožňuje seskupovat provozní záznamy HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity. Dále požadujeme přehledné webové rozhraní pro vyhledávání, přizpůsobitelné reporty a statistiky, tak aby Log Management usnadnil práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

Požadovaná funkcionalita	Specifikace minimálních požadavků
Forma obsluhy	Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní.
Počet podporovaných zdrojů log. událostí	**500 IP adres**

Komponenta Log Managementu musí mít garantovanou licenci pro:	**Zpracování 250 EPS nebo 10 GB/day**
Provedení	**Virtuální appliance: Pro účely navrženého řešení budou zadavatelem poskytnuty zdroje na jeho virtuální platformě.**
Podpora vstupních protokolů (sources ~ zdrojů log záznamů) a přenosu dat.	SNMP, syslog: - UDP (dle RFC 3164), - TCP, - IETF (RFC 5424) + TLS
Aktivní sběr logů z databází.	přes ODBC, minimálně MSSQL, MYSQL, ORACLE
Podpora BUFFER/CACHE na výstupu jak u Agenta, tak pro RELAY, a také pro Server/Appliance.	
Podpora výstupních protokolů (destinations ~ umístění log záznamů).	syslog (UDP, TCP, IETF). zápis logových dat napřímo do databází (ODBC). zápis logových dat do JSON formátu. SNMP Trap.
Řízení přístupů (AAA) - řízení přístupu na úrovni jednotlivých úložišť (logspace).	
Zálohování, Archivace, Export, Sdílení log dat	Nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace). Nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat. Podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru.
Rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů).	Velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích.
Možnost vyhledávání přes REST API rozhraní.	
Všechny potřebné komponenty HW i SW musí být součástí dodaného systému LM, včetně databáze.	
Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím MS EDGE a novějších, nebo jiným podobným způsobem. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X.	
Systém LM musí umožňovat přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD.	
Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nesmí být vázány na AD, musí být spravovány interně.	Vrstva sběru logů musí podporovat načítání logů z databáze (zejména Microsoft SQL a Oracle), kde tyto logy budou mít stanovenu strukturu a význam dat.
Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup) a samostatných oddělených logspace.	

Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat.	
Systém LM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat.	
Komponenta sbírající logy, musí být schopna trvale zpracovávat 10000 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení.	
Komponenta Log Managementu musí mít garantovaný výkon pro zpracování 10000 EPS.	
Systém dále musí umožnit uchovávání logů formou záloh a zejména musí umožnit obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu LM.	
Licence musí obsahovat možnost minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí, atd).	
Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů událostí a vlastních custom logů.	
Vrstva sběru logů musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenu strukturu a význam dat.	
Vrstva sběru logů musí podporovat načítání logů z databáze (zejména Microsoft SQL a Oracle), kde tyto logy budou mít stanovenu strukturu a význam dat.	
Vrstva sběru logů musí umožňovat načtení a zpracování jakýchkoli typů logů, i z vlastních aplikací, tato možnost musí být k dispozici bez součinnosti výrobce nebo dodavatele řešení. Kvalita výstupu a možnosti využití musí být stejné jako v případě standardně podporovaného zdroje logů.	
Komponenta sbírající logy je musí posílat dále zašifrované a komprimované a musí umožňovat regulovat šířku užívaného pásma.	
LM systém musí podporovat pravidelné automatické přesuny dat z interního do externího úložiště, resp. archivu podle definovaných pravidel, a bez vzniku neautorizovaných změn dat;	
LM musí ukládat data v komprimované podobě pro úsporu diskové kapacity, a to v rámci interního i externího úložiště;	
LM systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu;	
LM systém musí poskytovat mechanismus detekce neautorizovaných změn dat (kontrola integrity) v souborech systému LM;	
Systém LM musí poskytovat reporty i ve formě grafů a tabulek.	
Systém LM musí vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.	
Systém LM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.	
Systém LM musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzn. raw-message.	
Systém LM musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	
Řešení poskytuje funkci event. managementu (práce s událostmi ve formě strukturovaných eventů)	Součástí dodávky je sada parserů pro obvyklá zařízení klasických ICT výrobců

Vrstva sběru (zpracování, parsování, normalizace,…) je logicky i fyzicky oddělená od centrální komponenty LM (server zajišťující uložení a vyhledávání)	
Záruka a servisní podpora	**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.**

Příloha č. 3: Cenový rozpočet

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha č. 3 ZD Cenový rozpočet

Název zakázky: DODÁVKA FIREWALLU A LOG MANAGEMENTU

Název položky	**Cena bez DPH**	**Výše DPH**	**Cena s DPH**
1. Next generation firewall (NGFW)			
Fortinet FG-120G	103 068,8,-	21 644,4,-	124 713,2,-
Servisní podpora na 5 let	171 460,8,-	36 006,8,-	207 467,6,-
2. Webový aplikační firewall (WAF)			
Fortinet FG-120G	Součástí ceny za NGFW		
Servisní podpora na 5 let			
3. Log management			
Log management	317 528,-	66 680,9,-	384 208,9,-
Servisní podpora na 5 let	793 380,-	166 609,8,-	959 989,8,-
Celková nabídková cena za jednotlivé položky a poskytování služeb technické podpory (součet pol.1 až 3)	1 385 437,6,-	290 941,9,-	1 676 379,5,-

Příloha č. 4 Náležitosti poskytování servisních zásahů

1. FIREWALL

FortiCare Premium je úroveň podpory od Fortinetu, která nabízí **rozšířené služby** oproti standardním úrovním (jako je FortiCare 24x7). Je navržena pro zákazníky, kteří potřebují rychlejší řešení incidentů a proaktivnější přístup k podpoře.

Hlavní vlastnosti a výhody FortiCare Premium typicky zahrnují:

- **24x7 technická podpora:** Přístup k technické podpoře (TAC - Technical Assistance Center) 24 hodin denně, 7 dní v týdnu, 365 dní v roce, prostřednictvím webu (portálu), chatu a telefonu.

Kam se hlásí požadavky (otevírání ticketů)?

Požadavky na podporu (otevírání ticketů) se u Fortinetu hlásí primárně přes **Fortinet Support Portal**.

Postup pro podání požadavku:

1. **Přihlášení na Fortinet Support Portal:**
   - Jděte na https://support.fortinet.com.
   - Přihlaste se pomocí svého účtu FortiCloud/FortiCare. Tento účet musí být spojen s vašimi produkty, které mají aktivní FortiCare Premium licenci.
2. **Vytvoření nového ticketu:**
   - Po přihlášení obvykle najdete možnost "Create a Ticket" (Vytvořit ticket) v navigačním menu (často pod "Support" nebo "Tickets").
   - Budeš vyzván(a) k zadání informací, jako jsou:
     - **Serial Number (Sériové číslo) zařízení:** Toto je klíčové, protože podle něj systém ověří, jakou úroveň FortiCare podpory máte.
     - **Typ požadavku:** Technická podpora, RMA (výměna hardwaru), dotaz na licenci atd.
     - **Kategorie problému:** Např. Network, Security, VPN, FortiClient, FortiSwitch, atd.
     - **Předmět a popis problému:** Zde je důležité uvést co nejpodrobnější informace o problému, kroky k reprodukci, chybové zprávy, logy, topologii sítě atd. Čím více informací poskytneš, tím rychleji Fortinet TAC může začít s řešením.
     - **Kontakt a preference:** Kontaktní údaje a preference pro komunikaci (telefon, e-mail).
     - **Priorita:** U FortiCare Premium budete mít možnost nastavit vyšší priority pro kritické problémy, s odpovídajícími SLA.
3. **Další možnosti komunikace (pro FortiCare Premium):**
   - **Telefonický kontakt:** Pro kritické problémy můžete zavolat přímo na Fortinet TAC, přičemž budete potřebovat sériové číslo zařízení pro ověření podpory. Telefonní čísla se liší podle regionu a jsou k dispozici na support portálu.

     Mezinárodní číslo pro Technickou Podporu (TAC):

   - (Toto je mezinárodní číslo do Fortinet Support Centra).

- Pro volání z České republiky budete muset vytočit příslušný mezinárodní předvolbu (např. 00 nebo +).
- **Online Chat:** Pro méně kritické dotazy nebo rychlé konzultace je často k dispozici online chat s technickou podporou.

2. Log Management

Poskytování Servisní podpory na LM je **formou vzdáleného přístupu**

Servisní kontakty:

- Telefonicky na čísle: +420
- E-mailem na adrese:

Rozsah poskytování služeb

- Podpora zahrnuje všechny updaty i upgrady
- Telefonická nebo emailová podpora výrobce v rozsahu 8x5 (8:00 – 16:00).
- Přijetí požadavku: 4 hodiny v pracovní dobu
- Zahájení řešení: NBD