KUPNÍ SMLOUVA

uzavřená níže uvedeného dne, měsíce a roku

dle ustanovení § 2079 a násl. a § 2085 a násl. zákona č. 89/2012 Sb., Občanského zákoníku, v platném znění

Číslo smlouvy: 51092024

Čl. 1 Smluvní strany

Kupující: Plzeňský kraj

Sídlo:	Škroupova 18, 306 13 Plzeň
IČO:	70890366
DIČ:	CZ70890366
Zastoupený:	MUDr. Kamalem Farhanem, hejtmanem Plzeňského kraje
K podpisu smlouvy oprávněn:	Mgr. Štěpánka Szabó, MBA, ředitelka Krajského úřadu Plzeňského kraje, na základě Podpisového a kompetenčního řádu PK a KÚPK
Kontaktní osoba:	[redacted] odbor informatiky, Krajský úřad Plzeňského kraje,
e-mail:	[redacted]
Bankovní spojení:	Raiffeisenbank a.s., pobočka Plzeň
Číslo účtu:	1063003350/5500

jako kupující na straně jedné (dále jen kupující, objednatel)

a

Prodávající: Aricoma Systems a.s.

Sídlo:	Hornopolní 3322/34, 702 00 Ostrava
IČO:	04308697
DIČ:	CZ04308697
Zastoupený/Jednající:	[redacted] ředitelem regionálního centra
Kontaktní osoba:	[redacted] ředitel regionálního centra
Bankovní spojení:	[redacted]
Číslo účtu:	

Zápis v OR: vedený u Krajského soudu v Ostravě, spisová značka B/11012

jako prodávající na straně druhé (dále také prodávající, dodavatel)

Čl. 2 Úvodní ustanovení

2.1. Tato smlouva se uzavírá na základě vyhodnocení veřejné zakázky malého rozsahu s názvem Bezpečnostní IPS sonda (Appliance pro analýzu a blokování síťového provozu), realizované veřejným zadavatelem Plzeňský kraj v souladu s jeho interním předpisem.

2.2. Technické požadavky kupujícího (Technická dokumentace zadavatele) k veřejné zakázce a technická konfigurace z nabídky prodávajícího tvoří nedílnou součást této smlouvy jako její přílohy.

Čl. 3 Specifikace plnění

3.1. Detailní technická specifikace předmětu plnění této smlouvy je obsažena v přílohách č. 1 a č. 2, které tvoří nedílnou součást této smlouvy.

3.2. Prodávající prohlašuje, že:

- Dodávané zboží je ke dni jeho dodání nové, originální, nepoužité, nerepasované, určené pro český trh. V databázi výrobce, pokud taková existuje, bude kupující veden jako první uživatel zboží.
- Veškeré, prodávajícím deklarované funkce a technické parametry předmětu dodávky, jsou dostupné realizací dodávky.

Čl. 4 Předmět smlouvy

4.1. Předmětem plnění této smlouvy je

a) dodávka 2 ks bezpečnostní IPS sondy (HW) včetně licence k předmětnému hardware,

b) on-site instalace dodaných 2 ks IPS sondy do racků v rámci určeného technického prostředí kupujícího (Technologické centrum Plzeňského kraje),

c) poskytnutí běžné/standardní záruky a podpory,

d) poskytnutí tzv. rozšířené záruky na 7 let a technické podpory HW v režimu NBD (tj. Next Business Day) on-site,

vše dle technické specifikace uvedené v přílohách č. 1 a 2 této smlouvy.

4.2. Prodávající se zavazuje dodat předmět smlouvy kupujícímu s veškerými doklady nutnými k převzetí a zejména k užívání dodaného hardware.

4.3. Prodávající touto smlouvou prodává kupujícímu do výlučného vlastnictví předmět smlouvy definovaný v čl. 3 smlouvy.

4.4. Kupující předmět plnění této smlouvy, jímž jsou věci nové a nepoužité, kupuje za dohodnutou kupní cenu a přijímá do svého výlučného vlastnictví.

4.5. Prodávající prohlašuje, že neví ke dni podpisu této kupní smlouvy o žádných vadách prodávaných movitých věcí, na které by kupujícího upozornil.

4.6. Kupující prohlašuje, že prodávající předložil před uzavřením této smlouvy kopii pojistné smlouvy (pojistného certifikátu) o minimální pojistné částce 2.000.000 Kč, jejímž předmětem je pojištění odpovědnosti za škody způsobené při výkonu podnikatelské činnosti.

Čl. 5 Licence

5.1. Prodávající v rámci plnění předmětu této smlouvy dodává software podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon) a ustanovení § 2358 a následující zákona č. 89/2012, občanského zákoníku, proto poskytuje kupujícímu licenci (tj. oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném rozsahu), a to formou licenčního ujednání v této kupní smlouvě. Prodávající prohlašuje, že se jedná o licenci:

a) nevýhradní licenci k veškerým známým způsobům užití takového díla, a to v rozsahu minimálně nezbytném pro řádné užívání díla kupujícím;
b) licenci neomezenou územním či množstevním rozsahem a rovněž tak neomezenou způsobem nebo rozsahem užití;
c) licenci udělenou na dobu určitou,
d) licenci převoditelnou a postupitelnou, tj. která je udělena s právem postoupení licence třetí osobě
e) licenci, kterou není kupující povinen využít.

5.2. Prodávající prohlašuje, že odměna za poskytnutí licence kupujícímu je již zahrnuta v kupní ceně za poskytnuté plnění dle této kupní smlouvy.

Čl. 6 Kupní cena a platební podmínky

6.1. Kupní cena je nabídkovou cenou předloženou prodávajícím v jeho nabídce na veřejnou zakázku malého rozsahu s názvem Bezpečnostní IPS sonda (Appliance pro analýzu a blokování síťového provozu), resp. v e-aukci.

6.2. Kupující se zavazuje zaplatit prodávajícímu za předmět plnění uvedený v čl. 3 a 4 této smlouvy kupní cenu ve výši 1 990 000 Kč bez DPH.

6.3. K uvedené ceně bude připočtena daň z přidané hodnoty ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

6.4. Kupní cena zahrnuje veškeré dodávky a služby s dodávkami související a veškeré jiné náklady nezbytné pro řádnou a úplnou realizaci předmětu plnění této smlouvy včetně všech rizik a vlivů s plněním předmětu této smlouvy souvisejících.

6.5. Prodávající není oprávněn požadovat po kupujícím poskytnutí zálohy.

6.6. Kupující je oprávněn, dle disponibilnosti finančních prostředků, iniciovat vystavení zálohové faktury na předmětné plnění až do výše 100% kupní ceny.

6.7. Prodávající na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy.

6.8. Kupní cenu zaplatí kupující prodávajícímu bankovním převodem na bankovní účet na základě daňového dokladu (faktury) vystaveného prodávajícím ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu na předmět plnění dle této smlouvy.

6.9. Daňový doklad je považován za proplacený okamžikem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.

6.10. Na daňovém dokladu (faktuře) bude uveden rozklad fakturované částky na jednotlivá zařízení, tak aby byla zřejmá cena jednotlivých zařízení a tak, aby bylo objednateli usnadněno zavedení do majetkové evidence.

6.11. Splatnost daňového dokladu činí 30 dnů ode dne jeho doručení kupujícímu do elektronické podatelny na posta@plzensky-kraj.cz (elektronická faktura).

6.12. Daňový doklad bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude mít náležitosti obchodní listiny dle § 435 zákona č. 89/2012 Sb., občanského zákoníku. V případě, že daňový doklad takové náležitosti nebude splňovat, bude kupujícím vrácen do dne splatnosti daňového dokladu k opravení bez jeho proplacení. V takovém případě lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nového vyhotovení daňového dokladu.

Čl. 7 Místo a čas plnění, převzetí a předání

7.1. Prodávající předá kupujícímu předmět plnění této smlouvy (2 ks IPS sondy) do čtyř (4) kalendářních týdnů od účinnosti kupní smlouvy jejím uveřejněním v informačním systému Registru smluv. Místem plnění pro dodávku a instalaci je Technologické centrum Plzeňského kraje na adresách Škroupova 18, Plzeň (TC1) a U Hasičů 1, Plzeň – Košutka (TC2). Instalaci 2 ks IPS sondy do Technologického centra Plzeňského kraje (2 místa) provede dodavatel nejpozději do 4 měsíců od účinnosti smlouvy na plnění VZ.

7.2. Vlastnické právo k HW (2 ks IPS sondy) přechází na kupujícího v okamžiku jeho předání a převzetí, potvrzeném na předávacím protokolu.

7.3. Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností předmětu plnění včetně užitku přechází na kupujícího současně s nabytím vlastnictví.

7.4. Náklady spojené s předáním předmětu plnění, zejména dopravu, nese prodávající a náklady spojené s převzetím nese kupující.

7.5. O předání a převzetí předmětu plnění a souvisejících dokladů bude sepsán předávací protokol podepsaný zástupci oběma smluvních stran. O instalaci 2 ks IPS sondy do technického prostředí kupujícího bude sepsán akceptační protokol. Za kupujícího je předávací/akceptační protokol oprávněn podepsat a předmět plnění převzít [redacted] vedoucí oddělení správy serverů a sítě, odbor informatiky, Krajský úřad Plzeňského kraje.

7.6. Podkladem pro vystavení faktury (daňového dokladu) je akceptační protokol osvědčující instalaci IPS sondy (2 ks) do určeného technického prostředí kupujícího.

7.7. Pokud prodávající předmět plnění nedoručí vlastními prostředky, ale využije k tomu dopravce, považuje se za odevzdání věci kupujícímu až okamžik doručení takovým dopravcem. Ustanovení § 2090 a § 2091 zákona č. 89/2012 Sb., občanského zákoníku, se nepoužijí.

Čl. 8 Záruka a záruční servis

8.1. Prodávající poskytuje kupujícímu záruku po dobu 7 let od akceptace instalace IPS sondy (2 ks) do určeného technického prostředí kupujícího (Škroupova 18, Plzeň (TC1) a U Hasičů 1, Plzeň – Košutka (TC2)) a zavazuje se poskytovat kupujícímu technickou podporu 2 ks IPS sondy v režimu NBD (next bussines day) po dobu 7 let od akceptace instalace IPS sondy do technického prostředí kupujícího.

8.2. Prodávající odpovídá kupujícímu za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, stanovené v minimální konfiguraci v technické dokumentaci kupujícího a v konečné konfiguraci v nabídce prodávajícího a že je bez právních a faktických vad. Dále prodávající zaručuje, že na dodaném předmětu smlouvy neváznou práva třetích osob.

8.3. Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.

8.4. Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.

Čl. 9 Smluvní pokuty

9.1. V případě prodlení se zaplacením kupní ceny se kupující zavazuje uhradit prodávajícímu smluvní pokutu ve výši 0,05 % z fakturované ceny bez DPH za každý den prodlení.

9.2. V případě prodlení prodávajícího s plněním předmětu smlouvy, v rozsahu a termínu uvedených v této smlouvě, se prodávající zavazuje uhradit kupujícímu smluvní pokutu ve výši 0,05 % kupní ceny bez DPH za každý den prodlení.

9.3. V případě prodlení prodávajícího s poskytnutím záručního servisu (technické podpory) v termínu a způsobem dle bodu 8.1. smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 300,- Kč bez DPH za každou, i započatou, hodinu prodlení prodávajícího, max. však do výše 100% ceny dodávky bez DPH.

9.4. Zaplacením smluvní pokuty nezaniká povinnost druhé strany závazek splnit a není tím dotčeno právo poškozené strany na náhradu škody, která nesplněním povinnosti vznikla.

9.5. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30-ti dnů od doručení jejího vyúčtování.

Čl. 10 Odstoupení od smlouvy

10.1. Odstoupení od smlouvy se řídí ustanoveními § 2001 a násl. zákona č. 89/2012 Sb., občanského zákoníku.

10.2. Nebude-li uhrazena kupní cena do 60 dnů ode dne splatnosti daňového dokladu, sjednává si prodávající právo odstoupit od této kupní smlouvy.

10.3. Právo odstoupit od této kupní smlouvy má kupující tehdy, jestliže jej prodávající ujistil, že předmět plnění této smlouvy má určité vlastnosti, zejména vlastnosti kupujícím vymíněné, anebo prodávající kupujícího ujistil, že předmět plnění této smlouvy nemá žádné vady, a toto ujištění se ukáže být nepravdivým.

10.4. Právo okamžitě odstoupit od této kupní smlouvy má kupující tehdy, jestliže se ukáže jako nepravdivé kterékoliv tvrzení z čestného prohlášení prodávajícího, uvedeného v bodě 3.2. smlouvy.

Čl. 11 Zvláštní povinnosti prodávajícího

11.1. Dodavatel se zavazuje zajišťovat důstojné pracovní podmínky, bezpečnost práce a důsledně dodržovat všechny pracovněprávní předpisy, zejména pak zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů a zákon č. 435/2004 Sb., o

zaměstnanosti, ve znění pozdějších předpisů, a to ve vztahu ke všem osobám, které zaměstnává a rovněž k osobám, které se budou podílet na předmětu plnění veřejné zakázky.

11.2. Dodavatel se zavazuje přijímat v rámci řádného plnění předmětu veřejné zakázky vhodná opatření k ochraně životního prostředí, předcházet znečišťování a poškozování životního prostředí, zejména využívat pro komunikaci a korespondenci prostředky elektronické komunikace, minimalizovat spotřebu kancelářského materiálu, používat výrobky z recyklovaného materiálu apod.

Čl. 12 Závěrečná ustanovení

12.1. Tato Smlouva je vyhotovena v elektronické podobě v 1 vyhotovení s elektronickými podpisy obou smluvních stran, v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

12.2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem zveřejnění uzavřené smlouvy v Registru smluv.

12.3. Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, v platném znění.

12.4. Smluvní strany berou na vědomí, že uzavřená smlouva, včetně všech případných dodatků, bude uveřejněna v informačním systému Registru smluv. Splnění této zákonné povinnosti zajistí strana kupující (Plzeňský kraj).

12.5. Nedílnou a závaznou součástí této smlouvy jsou její přílohy:

- Příloha č. 1 – Technická dokumentace zadavatele /technické požadavky kupujícího/
- Příloha č. 2 – Technická konfigurace dodavatele /technické řešení z nabídky prodávajícího/

12.6. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují podpisy na smlouvě.

Za kupujícího	**Za prodávajícího**
Mgr. Štěpánka Szabó, MBA ředitelka Krajského úřadu Plzeňského kraje	[redacted] ředitel regionálního centra Aricoma Systems a.s. na základě plné moci
(podepsáno elektronicky)	(podepsáno elektronicky)

[redacted]

Příloha č. 1 smlouvy – Technická specifikace kupujícího (Technická dokumentace zadavatele)

Příloha č. 1 výzvy - Technická dokumentace zadavatele

Požadavek
minimální počty a rychlosti portů, 8x 10GE SFP+ port, 4x 1GE port RJ45 nebo SFP; z toho tři porty SFP+ budou obsahovat SR trancievery vhodné pro zařízení
Minimální garantovaná propustnost SSL 5Gps, velikost klíčů min. 2048, počet spojení za sekundu min. 5000;TLS provoz v1.2 nebo v1.3 na L2
L3 propustonst zařízení alespoň 70GB (při velikosti udb/tcp paketů 64byte)
Minimální garantovaná propustnost IP se zapnutou funkcí ochrany 12Gps v běžném firemním provozu(kombinace různých protokolů)
Podporované nasazení senzoru (také podpora pro port clustering nebo High-availability):
- SPAN nebo Hub
- Tap
DoS profily: 300
Latence méně než 100 mikrosekund v běžném provozu
Senzor využívá dedikovaný LAN Management port pro komunikaci s "Manager serverem", podpora IPv4 a IPv6
Oddělený minimálně log managment a reporting SW od sondy nebo garance, že práce logmanagementem v sondě nebude mít dopad na výkon sondy. Lze očekávat, že logy mohou mít řádově 10GB denně a dotazy/reporty mohou být měsíční, různě komplikované, tedy výkonově náročné.
Možnost zasílat dešifrovaný SSL provoz k další analýze jiným HW/SW produktům po síti LAN
Možnost "High Availability" řešení, obnovy po havárii pro nepřetržitý vysoký výkon(postačí Active/passive)
Zařízení Intrusion Prevention System (IPS) filtruje v reálném čase síťový provoz a podle stanovené politiky blokuje nebo upozorňuje na provoz, který by mohl být hrozbou pro vnitřní stroje a infrastrukturu.
Chrání prostředí před známými i neznámými hrozbami pomocí hloubkové inspekční technologie (kombinace úplné analýzy protokolu, reputačního hodnocení hrozeb a behaviorální analýzy podezřelého chování), ochrana proti útokům typu callbacks, Dos, Zero-day aj.
Jako reakce na vzniklou událost je možné použít zaslání záznamu do syslogu.
V IPS jsou obsaženy/aktualizovány signatury pro pokrytí OWASP top 10 útoků.
Pravidelné aktualizace IPS signatur od výrobce (min. automatické)
Analýza provozu a signatury vztahující se na detekci a prevenci komunikace botnetů. Tyto signatury jsou minimálne 1x denne aktualizovány.
V případě budoucího použití více sond možnost jednotné správy těchto IPS sond
Přehled o konkrétních aplikacích
Nepřetržitá aktualizace systému díky globální síti laboratoří
Odlišné politiky na základě směru provozu
Rozpoznávání jednotlivých aplikací a vizualizace
Možnost integrace s malware sandboxem
Funkcionalita SYN cookies pro zajištění ochrany proti nadměrnému navazování spojení.
ochrana IP spoofing
Inspekce IPv6 provozu
Inspekce tunelovaného provozu (včetně provozu GRE)
Podpora dekomprese odezvy HTTP
Monitoring latence obecně
Monitorování výkonu senzoru
Možnost Whitelistů a Blacklistů
Zobrazení událostí protokolu monitorování senzorů CLI v manageru
Zabezpečený přenos souborů ze senzoru CLI
Inspekce SSL provozu = dešifrování TLS v1.2 a v1.3 na L2 - podpora MS Windows a Linux serverů(za předpokladu nahrání privátních klíčů do IPS), metody DHE, ECDHE
IPS politiky

Pravidla přístupu k managementu IPS (ACL na L3, L4)
Rozpoznávání a ochrana na aplikační vrstvě 7 OSI modelu (například detekce shellcode v přenášených souborech a jejich hodnocení pomocí online anti-malware služby, kategorizace webů podle URL)
Možná anti-malware kontrola dat procházejících sondou po známých protokolech (např. Http, smtp) s následní real-time blokací nebo identifikací viru a vytvoření události.
DNS DoS ochrana(alespoň na úrovni počtu udp session)
IPS politiky pro exploit útoky
IPS poskytuje obecně podporu proti DoS útokům (Skrz předdefinované politiky nebo možnosti vytvářet vlastní na základě aktuálního provozu).
Politiky pro omezení síťového provozu
Možnost vytváření vlastních IPS signatur
Možnost integrace s globální reputační databází (reputaci IP a souborů) a integrace s geolokační databází. IPS umí na daný hodnocený provoz reagovat či využít reputaci/geolokaci jako atribut pro vytvoření pravidel.
Karanténa (automatická, k dispozici skrz IPS politiky, z logu, samostatné záložky konzole).
SmartBlocking(časově omezené blokování) útoků včetně možnosti použití IP Reputation pro rozšíření SmartBlocking
Simulace blokování (možnost funkce simulace blokování, která umožňuje umístit senzor do neblokujícího režimu, kdy útoky nejsou blokovány, i když je k tomu nakonfigurovaná aplikovaná politika IPS.)
Zachycení datových paketů s možností zobrazení (pro kliknutím z GUI na externí program WireShark nebo analogický produkt/funkcionalitu pro analýzu obsahu paketů)
Řízení přístupu (podpora například TACACS)
Ochrana webového serveru před útoky DoS
Generování a export Netflow v9 nebo IPFIX na vybrané zařízení pro analýzu
Ochrana vůči útokům za použití evasion techniky.
Detekce Zero-Day javascript hrozeb v PDF souborech
IPS umožní alespoň pět virtuálních instancí
Základní zaškolení formou instalace a nastavení sondy. Vytvoření dvou virtuálních instancí ostré a testovací. Součinnost při prvotním ladění sondy do provozu(v průběhu dvou měsíců opakované kontrolní meetinky 1h/týdně, kdy se vyhodnotí provoz a nastaví vhodné politiky)
7let podpory - nárok na nové verze SW, bezpečnostní signatury, servis HW on-site NBD
Požadujeme dodávku sondy formou HW appliance a SW managementu od jednoho výrobce, záruka a servis od jednoho výrobce na celek po dobu 7 let NBD .
Základní zaškolení formou instalace a nastavení sondy.
Dále v horizontu 2 let(zatím není stanoven termín) bude zapotřebí nasadit řešení automatické výměny certifikátů v součinnosti s organizací CESNET(součinnost zajistí zadavatel). Tento specifický úkon zařazujeme do podpory a ceny této dodávky, kdy úkon může provést dodavatel.

Příloha č. 2 - Technická konfigurace dodavatele (technické řešení z nabídky prodávajícího)

2ks FortiGate 400F HW, Licence, Unified Threat Protection + FortiCare Premium + FortiAnalyzer VM Subscription, FortiAnalyzer-VM Subscription License

Požadavek	Popis nebo přesný odkaz na dokumentaci, vč. kapitoly, čísla stránky apod.
minimální počty a rychlosti portů, 8x 10GE SFP+ port, 4x 1GE port RJ45 nebo SFP; z toho tři porty SFP+ budou obsahovat SR trancievery vhodné pro zařízení	8x 10GE SFP+, 16x 1GE RJ45, 8x 1GE SFP; 3x Fortinet FN-TRAN-SFP+SR
Minimální garantovaná propustnost SSL 5Gps, velikost klíčů min. 2048, počet spojení za sekundu min. 5000;TLS provoz v1.2 nebo v1.3 na L2	8Gps, velikost klíčů min. 2048 - ano, počet spojení za sekundu 800 tis.
L3 propustonst zařízemí alespoň 70GB (při velikosti udb/tcp paketů 64byte)	70GB - UDP 64B
Minimální garantovaná propustnost IP se zapnutou funkcí ochrany 12Gps v běžném firemním provozu(kombinace ruzných protokolů)	IPS Throughput 12Gps, 78Gps v běžném IP provozu
Podporované nasazení senzoru (také podpora pro port clustering nebo High-availability):	
- SPAN nebo Hub	Ano - Virtual wire viz. FortiOS-7.6.0-Administration_Guide.pdf
- Tap	Ano - One-arm sniffer viz. FortiOS-7.6.0-Administration_Guide.pdf
DoS profily: 300	Ano, podporováno je 512 politik celkem a maximálně 256 per VDOM (koukal jsem na 80F a 120F, vyšší platforma jich bude mít podporovaných minimálně stejně). Údaj nelze nalézt v dokumentaci, lze ho zobrazit v CLI FW (print tablezise, parametr - firewall.DoS-policy: 0 256 512.)
Latence méně než 100 mikrosekund v běžném provozu	4.19 µs
Senzor využívá dedikovaný LAN Management port pro komunikaci s "Manager serverem", podpora IPv4 a IPv6	Ano, na jakémkoliv portu
Oddělený minimálně log managment a reporting SW od sondy nebo garance, že práce logmanagementem v sondě nebude mít dopad na výkon sondy. Lze očekávat, že logy mohou mít řádově 10GB denně a dotazy/reporty mohou být měsíční, různě komplikované, tedy výkonově náročné. Minimálně management logů je očekáván formou virtuální appiliance do našeho prostředí(požadované výkonostní parametry prostředí zajistí zadavatel)	Ano - 10GB logů denně
Možnost zasílat dešifrovaný SSL provoz k další analýze jiným HW/SW produktům po síti LAN	Ano - SSL offloading viz. FortiOS-7.6.0-Administration_Guide.pdf
Možnost "High Availability" řešení, obnovy po havárii pro nepřetržitý vysoký výkon(postačí Active/passive)	Ano - Active-Active, Active-Passive, Clustering
Zařízení Intrusion Prevention System (IPS) filtruje v reálném čase síťový provoz a podle stanovené politiky blokuje nebo upozorňuje na provoz, který by mohl být hrozbou pro vnitřní stroje a infrastrukturu.	Ano -kombinace FortiGate a FortiAnalyzer

Chrání prostředí před známými i neznámými hrozbami pomocí hloubkové inspekční technologie (kombinace úplné analýzy protokolu, reputačního hodnocení hrozeb a behaviorální analýzy podezřelého chování), ochrana proti útokům typu callbacks, Dos, Zero-day aj.	Ano - je součástí nabízeného UTP balíčku
Jako reakce na vzniklou událost je možné použít zaslání záznamu do syslogu.	Ano - pomocí FortiAnalyzeru
V IPS jsou obsaženy/aktualizovány signatury pro pokrytí OWASP top 10 útoků.	Ano - IPS + WAF profil ve Fortigate
Pravidelné aktualizace IPS signatur od výrobce (min. automatické)	Ano - včetně Pusch notice od výrobce
Analýza provozu a signatury vztahující se na detekci a prevenci komunikace botnetů. Tyto signatury jsou minimálne 1x denne aktualizovány.	Ano
V případě budoucího použití více sond možnost jednotné správy těchto IPS sond	Ano - FortiManager
Přehled o konkrétních aplikacích	Ano - pomocí Aplikační kontroly
Nepřetržitá aktualizace systému díky globální síti laboratoří	Ano
Odlišné politiky na základě směru provozu	Ano - zones viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Rozpoznávaní jednotlivých aplikací a vizualizace	Ano - pomocí Aplikační kontroly
Možnost integrace s malware sandboxem	Ano - pomocí Forti SandBoxem
Funkcionalita SYN cookies pro zajištění ochrany proti nadměrnému navazování spojení.	Ano - Dos policy profil - viz výše
ochrana IP spoofing	Ano - Reverse path look-up viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Inspekce IPv6 provozu	Ano - datasheet
Inspekce tunelovaného provozu (včetně provozu GRE)	Ano - inspekce tunelovaného provozu je podporována. V tomto dokumentu je zmínka o detekci tunelovaných aplikací v sekci o dekodérech. https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortigate-visibility.pdf
Podpora dekomprese odezvy HTTP	Ano - podporováno, popsáno např. zde: https://docs.fortinet.com/document/fortigate/7.6.0/new-features/88133/support-the-zstandard-compression-algorithm-for-web-content
Monitoring latence obecně	Ano - s pomocí monitorovacích aplikací 3. stran nebo FortiManager
Monitorování výkonu senzoru	Ano - s pomocí monitorovacích aplikací 3. stran nebo FortiManager
Možnost Whitelistů a Blacklistů	Ano
Zobrazení událostí protokolu monitorování senzorů CLI v manageru	Ano - pomocí integrovaných diagnostických nástrojů
Zabezpečený přenos souborů ze senzoru CLI	Ano

Inspekce SSL provozu = dešifrování TLS v1.2 a v1.3 na L2 - podpora MS Windows a Linux serverů(za předpokladu nahrání privátních klíčů do IPS), metody DHE, ECDHE	Ano - konkrétní protokoly a šifry nejsou v dokumentaci u dešifrování SSL zmíněny, ale je to zcela jistě podporováno, ověřili jsme to nezávisle v labu.
IPS politiky	Ano - policy a profiles viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Pravidla přístupu k managementu IPS (ACL na L3, L4)	Ano - local-in policy viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Rozpoznávání a ochrana na aplikační vrstvě 7 OSI modelu (například detekce shellcode v přenášených souborech a jejich hodnocení pomocí online anti-malware služby, kategorizace webů podle URL)	Ano - funkcionality NG FW
Možná anti-malware kontrola dat procházejících sondou po známych protokolech (např. Http, smtp) s následní real-time blokaci nebo identifikaci viru a vytvoření události.	Ano - funkcionality NG FW
DNS DoS ochrana(alespoň na úrovni počtu udp session)	Ano - Traffic shaping viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
IPS politiky pro exploit útoky	Ano - policy a profiles viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
IPS poskytuje obecně podporu proti DoS útokům (Skrz předdefinované politiky nebo možnosti vytvářet vlastní na základě aktuálního provozu).	Ano - policy a profiles viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Politiky pro omezení síťového provozu	Ano - Traffic shaping viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Možnost vytváření vlastních IPS signatur	Ano - Configuring custom signatures viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Možnost integrace s globální reputační databází (reputací IP a souborů) a integrace s geolokační databází. IPS umí na daný hodnocený provoz reagovat či využít reputaci/geolokaci jako atribut pro vytvoření pravidel.	Ano - policy a profilesviz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Karanténa (automatická, k dispozici skrz IPS politiky, z logu, samostatné záložky konzole).	Ano - FortiAnalyzer automatizační akce
SmartBlocking(časově omezené blokování) útoků včetně možnosti použití IP Reputation pro rozšíření SmartBlocking	Ano - IP reputation filtering viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started
Simulace blokování (možnost funkce simulace blokování, která umožňuje umístit senzor do neblokujícího režimu, kdy útoky nejsou blokovány, i když je k tomu nakonfigurovaná aplikovaná politika IPS.)	Ano - Akci signatur lze přepnout z default na monitor režim (https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/583477/configuring-an-ips-sensor)
Zachycení datových paketů s možností zobrazení (pro kliknutím z GUI na externí program WireShark nebo analogický produkt/funkcionalitu pro analýzu obsahu paketů)	Ano - Using the packet capture tool viz. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started

Řízení přístupu (podpora například TACACS)	Ano - datasheet
Ochrana webového serveru před útoky DoS	Ano - policy a profiles viz. FortiOS-7.6.0-Administration_Guide.pdf
Generování a export Netflow v9 nebo IPFIX na vybrané zařízení pro analýzu	Ano - NetFlow - viz. FortiOS-7.6.0-Administration_Guide.pdf
Ochrana vůči útokům za použití evasion techniky.	Ano - v dokumentaci taková informace není, ale podporované to je. Ochrana před IPS evasion technikami, je ovšem zmíněna např. v tomto dokumentu https://www.fortinet.com/content/dam/fortinet/assets/resources/ser-fortiguard-ips.pdf
Detekce Zero-Day javascript hrozeb v PDF souborech	Ano - SandBox
IPS umožní alespoň pět virtuálních instancí	Ano - 10 VDOM
Základní zaškolení formou instalace a nastavení sondy. Vytvoření dvou virtuálních instancí ostré a testovací. Součinnost při prvotním ladění sondy do provozu(v průběhu dvou měsíců opakované kontrolní meetinky 1h/týdně, kdy se vyhodnotí provoz a nastaví vhodné politiky)	Ano - služby dle požadavků zákazníka
7let podpory - nárok na nové verze SW, bezpečnostní signatury, servis HW on-site NBD	Ano - součástí cenové nabídky
Požadujeme dodávku sondy formou HW appliance a SW managementu od jednoho výrobce, záruka a servis od jednoho výrobce na celek po dobu 7 let NBD .	Ano - součástí cenové nabídky
Základní zaškolení formou instalace a nastavení sondy.	Ano - služby dle požadavků zákazníka
Dále v horizontu 2 let(zatím není stanoven termín) bude zapotření nasadit řešení automatické výměny certifikátů v součinnosti s organizací CESNET(součinnost zajistí zadavatel). Tento specifický úkon zařazujeme do podpory a ceny této dodávky, kdy úkon může provést dodavatel.	Ano - služby dle požadavků zákazníka