Nabídka na uzavření Dílčí smlouvy č. 45

č. smlouvy Objednatele: MV-114775/OKT-2025

č. smlouvy Poskytovatele: 2025/141 NAKIT

dle ust. odst. 3.3 a 4.1 a násl. Rámcové dohody o integrovaných investičních dodávkách v oblasti informačních a komunikačních technologií,

č. smlouvy Objednatele: MV-186991/SIK5-2021 a

č. smlouvy Poskytovatele: 2022/080 NAKIT

(dále jen „Rámcová Dohoda“)

Nabídka je předkládána:

Národní agenturou pro komunikační a informační technologie, s. p.

se sídlem: Kodaňská 1441/46, 101 00 Praha 10
IČO: 04767543
DIČ: CZ04767543
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 77322
bankovní spojení: ČSOB a.s., č. ú: 117404973/0300
zastoupená: Mgr. Janem Ďoubalem, ředitelem
jako Poskytovatelem (dále jen „Poskytovatel“ nebo „NAKIT“)

pro:

Českou republiku – Ministerstvo vnitra

se sídlem: Nad Štolou 936/3, 170 34 Praha 7
IČO: 00007064
DIČ: CZ00007064
zastoupeno: Mgr. Romanem Novým, ředitelem odboru komunikačních technologií sekce informačních a komunikačních technologií

jako Objednatele (dále jen „Objednatel“ nebo „MV ČR“)
Poskytovatel a Objednatel společně dále též „Smluvní strany“

Dále jen „Nabídka“

1. Předmět Nabídky

Nabídka je předkládána na základě požadavku vedeného v CA SD pod ID 718473.

Předmětem Nabídky je návrh na uzavření Dílčí smlouvy dle ust. odst. 3.3 a čl. 4. Rámcové dohody na plnění spočívající v dodávce Náhrady IDS/IPS nástroje Trellix pro CMS2.0 (dále jen „IDS/IPS“).

Text Dílčí smlouvy č. 45 tvoří přílohu a nedílnou součást této Nabídky.

Akceptací Nabídky dochází k uzavření Dílčí smlouvy ve formě a rozsahu uvedené v příloze této Nabídky. Cena za plnění uvedená v Dílčí smlouvě je maximální a nepřekročitelná. Na základě poskytnutého plnění a stanovení konečných cen za poskytnuté dodávky a služby bude Smluvními stranami uzavřen dodatek k dílčí smlouvě.

2. Platnost nabídky

Nabídka je platná po dobu 30 dní, pokud nebude dohodnuto jinak.

3. Předkládá za Poskytovatele

V Praze dne dle el. podpisu

Jan Ďoubal

Digitálně podepsal Jan Ďoubal
Datum: 2025.11.28 14:39:36 +01'00'

Mgr. Jan Ďoubal, ředitel

Národní agentura pro komunikační a informační technologie, s. p.

4. Akceptace Návrhu řešení ze strany Objednatele

V Praze dne dle el. podpisu

……

Mgr. Romanem Novým, ředitelem odboru komunikačních technologií sekce informačních a komunikačních technologií **Ministerstvo vnitra České republiky**

Dílčí smlouva č. 45

Smluvní strany:

Česká republika – Ministerstvo vnitra
se sídlem: Nad Štolou 936/3, 170 34 Praha 7
IČO: 00007064
bank. spojení: Česká národní banka, pobočka Praha, Na Příkopě 28, 11503 Praha 1,
č. účtu: 3605-881/0710
zastoupená: Mgr. Romanem Novým, ředitelem odboru komunikačních technologií sekce informačních a komunikačních technologií

*(dále jen „**Objednatel**“ nebo „**MV ČR**“)*

a

Národní agentura pro komunikační a informační technologie, s. p.
se sídlem: Kodaňská 1441/46, Vršovice, 101 00 Praha 10
IČO: 04767543, DIČ: CZ04767543
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze,
pod spisovou značkou A 77322,
bank. spojení: Československá obchodní banka, a.s., č. účtu: 117404973/0300
zastoupená: Mgr. Janem Ďoubalem, ředitelem
*(dále jen „**Poskytovatel**“ nebo „**NAKIT**“)*
*(společně dále též „**Smluvní strany**“)*

Akceptací nabídky došlo k uzavření této Dílčí smlouvy č. 45 a to v souladu s čl. 3.3 a čl. 4. RÁMCOVÉ DOHODY o integrovaných investičních dodávkách v oblasti informačních a komunikačních technologií, č. smlouvy Objednatele: MV-186991/SIK5-2021 a č. smlouvy Poskytovatele: 2022/080 NAKIT (označené dále jen „Rámcová dohoda“).

Tato Dílčí smlouva č. 45 bude označována dále jako „Dílčí smlouva“.

1. Úvod a prohlášení Smluvních stran

1.1. *Poskytovatel poskytuje Objednateli plnění spočívající v dodávce služeb Poskytovatele specifikované v Nabídce (dále jen „Plnění“).*

2. Předmět Dílčí smlouvy

2.1. *Předmětem Dílčí smlouvy je dodávka Plnění spočívající v zajištění náhrady IDS/IPS nástroje Trellix pro CMS2.0. Bližší technická specifikace Plnění Dílčí smlouvy je uvedena v příloze 1 této Dílčí smlouvy.*

3. Způsob realizace Plnění

3.1. *Plnění bude realizováno vlastními zdroji NAKIT (Aktivity NAKIT) a prostřednictvím externího dodavatele (Externí dodávka).*

3.2. *Aktivity NAKIT spojené s realizací Plnění tvoří administrativní činnosti řízení a implementaci požadavku. Uvedené aktivity budou dodány v rámci tohoto maximálního rozsahu prací spojených s realizací řešení:*

Role	Celkem ČH/role	Popis činností
Specialista zákaznických řešení[1]	60	Sběr podkladů pro zpracování nabídky Dílčí smlouvy (DS), zpracování DS, vypořádání připomínek k DS, součinnost na přípravě VZ, administrativní činnosti.
Specialista obchodu senior[1]	15	Komunikace s Objednatelem. Administrativní činnosti spojené s řízením požadavku.
Bezpečnostní administrátor (3×)	112,5	Součinnost a řízení při implementaci nového řešení a deinstalaci současného končícího řešení. Zaškolení nového IPS/IDS nástroje.
Bezpečnostní architekt	15,0	Podklady do RFI, podklady do VZ, architektonické posouzení z hlediska bezpečnosti.
Projektový manažer	37,5	Koordinace postupu prací, řízení projektu a součinnost s externím dodavatelem a s uživatelem, akceptace Objednatelem, předání do provozní péče
Specialista datových sítí senior	45,0	Příprava adresního plánu, konfigurace a součinnost při nasazení IPS/ID sond a dekonfigurace stávajících sond. Ověření funkčnosti.
Specialista provozu senior	22,5	Příprava zálohy VM pro management, součinnost při povyšování verze nástroje pro management (2x VM, 1/DC)

[1] Role je součástí přímé výrobní režie Poskytovatele v souladu s příslušnou metodikou pro tvorbu cen dle posledního platného dodatku Smlouvy a představují část nákladů „back office zdrojů“, které se alokují přímo na danou aktivitu a zahrnují činnosti spojené se zpracováním Návrhu řešení, tj. příprava Návrhu řešení a administrativní činnosti spojené s řízením požadavku.

Role	Celkem ČH/role	Popis činností
Specialista nákupu senior[2]	*30*	*Příprava a realizace VZ na externí dodávku.*
Specialista legislativy senior	*37,5*	*Příprava a realizace výzvy a smluv k VZ.*
Projektový administrátor	*15*	*Příprava podkladů pro VZ, koordinace prací a součinnost s externím dodavatelem, sledování plnění úkolů, zpracování a aktualizace harmonogramu, vedení zápisů, vedení dokumentace projektu*
Teamleader (Dohledové centrum)	*15*	*Implementace a konfigurace nových sond do dohledového nástroje. Ověření funkčnosti.*
Analytik bezpečnostního dohledového centra	*37,5*	*Příprava podkladů do VZ, analýza při vyhodnocení VZ, součinnost při implementaci*
Architekt senior	*37,5*	*Návrhy změn zapojení, podklady do RFI, podklady do VZ, celkové architektonické posouzení.*
Specialista zákaznických požadavků	*5*	*Příprava a zpracování fakturace směrem k Objednateli a směrem k externímu dodavateli.*
Bezpečnostní architekt senior	*60*	*Podklady do RFI, podklady do VZ, architektonické posouzení z hlediska bezpečnosti*

3.3. Externí dodávku tvoří:

- *Dodávka IPS/IDS sond vč. licencí a montážního materiálu a služeb dle specifikace v příloze č. 1, podpory při implementaci a provozní dokumentace.*

4. Cena Plnění dle Dílčí smlouvy

4.1. Poskytovatel a Objednatel se dohodli, že cena Plnění dle Dílčí smlouvy, která Poskytovateli náleží za dodávku dle této Dílčí smlouvy, činí celkově ***10 631 783,50 Kč*** *bez DPH, tj.* ***12 864 458,04*** *s DPH.*

4.2. Celková cena plnění vychází z následujících částí:

Označení	Položka	Celkem bez DPH	DPH 21 %	Celkem vč. DPH
A	Aktivity NAKIT (A)	853 952,50 Kč	179 330,03 Kč	1 033 282,53 Kč
B	Externí dodávka (B)	9 777 831,00 Kč	2 053 344,51 Kč	11 831 175,51 Kč
Celkem		**10 631 783,50 Kč**	**2 232 674,54 Kč**	**12 864 458,04 Kč**

[2] Role je součástí administrativní přirážky Poskytovatele a představují část nákladů „back office zdrojů“, které se alokují přímo na danou aktivitu a zahrnují činnosti spojené s VZ dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek a zpracování příslušné smluvní dokumentace.

Jednotlivé položky (A, B) se skládají z:

Aktivity NAKIT (A)

Role	Cena role/MH bez DPH	Počet MH	Celková cena		
			Celkem bez DPH	DPH 21 %	Celkem s DPH
Specialista zákaznických řešení	*1 263 Kč*	*60,0*	*75 780,00 Kč*	*15 913,80 Kč*	*91 693,80 Kč*
Specialista obchodu senior	*1 440 Kč*	*15,0*	*21 600,00 Kč*	*4 536,00 Kč*	*26 136,00 Kč*
Bezpečnostní administrátor	*1 516 Kč*	*112,5*	*170 550,00 Kč*	*35 815,50 Kč*	*206 365,50 Kč*
Bezpečnostní architekt	*1 885 Kč*	*15,0*	*28 275,00 Kč*	*5 937,75 Kč*	*34 212,75 Kč*
Projektový manažer	*1 435 Kč*	*37,5*	*53 812,50 Kč*	*11 300,63 Kč*	*65 113,13 Kč*
Specialista datových sítí senior	*1 519 Kč*	*45,0*	*68 355,00 Kč*	*14 354,55 Kč*	*82 709,55 Kč*
Specialista provozu senior	*1 421 Kč*	*22,5*	*31 972,50 Kč*	*6 714,22 Kč*	*38 686,72 Kč*
Specialista nákupu senior	*1 438 Kč*	*30,0*	*43 140,00 Kč*	*9 059,40 Kč*	*52 199,40 Kč*
Specialista legislativy senior	*1 458 Kč*	*37,5*	*54 675,00 Kč*	*11 481,75 Kč*	*66 156,75 Kč*
Projektový administrátor	*1 156 Kč*	*15,0*	*17 340,00 Kč*	*3 641,40 Kč*	*20 981,40 Kč*
Teamleader	*1 694 Kč*	*15,0*	*25 410,00 Kč*	*5 336,10 Kč*	*30 746,10 Kč*
Analytik bezpečnostního dohledového centra	*1 562 Kč*	*37,5*	*58 575,00 Kč*	*12 300,75 Kč*	*70 875,75 Kč*
Architekt senior	*1 799 Kč*	*37,5*	*67 462,50 Kč*	*14 167,12 Kč*	*81 629,62 Kč*
Specialista legislativy senior	*1 458*	*37,50*	*54 675,00 Kč*	*11 481,75 Kč*	*66 156,75 Kč*
Specialista zákaznických požadavků senior	*1 217,00*	*5,0*	*6 085,00 Kč*	*1 277,85 Kč*	*7 362,85 Kč*
Bezpečnostní architekt senior	*2 182,00*	*60,00*	*130 920,00 Kč*	*27 493,20 Kč*	*158 413,20 Kč*
CELKEM – Aktivity NAKIT			***853 952,50 Kč***	***179 330,03 Kč***	***1 033 282,53 Kč***

Externí dodávka (B)

Popis komponenty	Cena / ks	Počet	Cena celkem bez DPH	DPH 21 %	Cena celkem s DPH
IPS/IDS sonda vč. implementace, podpory výrobcem a licence na 1 rok	*3 259 277,00 Kč*	*3*	*9 777 831,00 Kč*	*2 053 344,51 Kč*	*11 831 175,51 Kč*
Celkem - Externí dodávka			***9 777 831,00 Kč***	***2 053 344,51 Kč***	***11 831 175,51 Kč***

4.3. Smluvní strany se zavazují upravit cenu Plnění dle čl. 4.2. tak, že:

- *budou zohledněny skutečně vykonané činnosti ze strany NAKIT (položka „Aktivity NAKIT“);*
- *cena za „Externí dodávku“ bude odpovídat cenám uhrazeným Poskytovatelem externímu dodavateli/či dodavatelů.*

4.4. Součástí faktury za Dodávku HW (tj. IPS/IDS sondy) vč. implementační služby externího dodavatele a za konzultační služby externího dodavatele a za náklady NAKIT bude akceptační protokol, jehož nedílnou součástí je dodací list a faktura od externího dodavatele, aktivity report prací Poskytovatele a faktura od externího dodavatele.

4.5. Platební podmínky včetně podmínek fakturace jsou uvedeny v Rámcové dohodě, a to zejm. v čl. 8.

4.6. Smluvní strany se z důvodu změny legislativy dohodly, že pokud bude v okamžiku uskutečnění zdanitelného plnění správcem daně zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že Poskytovatel jako dodavatel zdanitelného plnění je nespolehlivým plátcem ve smyslu § 106a zákona o DPH, nebo že úplata za toto plnění má být poskytnuta zcela nebo zčásti bezhotovostním převodem na jiný účet než účet Poskytovatele, který je správcem daně zveřejněn, způsobem umožňujícím dálkový přístup ve smyslu ust. § 96 zákona o DPH, je příjemce zdanitelného plnění (Objednatel) oprávněn část ceny odpovídající dani z přidané hodnoty zaplatit přímo na bankovní účet správce daně ve smyslu ust. § 109a zákona o DPH. Na bankovní účet Poskytovatele bude v tomto případě uhrazena část ceny odpovídající výši základu daně z přidané hodnoty. Úhrada ceny plnění (základu daně) provedená Objednatelem v souladu s ustanovením tohoto odstavce Dílčí smlouvy bude považována za řádnou úhradu ceny plnění poskytnutého dle této Dílčí smlouvy.

5. Harmonogram plnění

5.1. Předpokládaný harmonogram Plnění je následující:

Část	Aktivita	Termín
1	Akceptace nabídky Dílčí smlouvy ze strany Objednatele	T0
2	Příprava VZ a smluvní zajištění externí dodávky	T1 = T0 + 4 týdnů
3	Dodávka HW a Instalace	T2 = T1 + 4 týdny
4	Implementace dodaného řešení a její předání do užívání	T3 = T2 + 12 týdnů
5	Akceptace a fakturace	T4 = T3+ 1 týdny

5.2. Zásadní změny harmonogramu budou upraveny dodatkem k této Dílčí smlouvě.

6. Požadavky na součinnost Objednatele

6.1. *Objednatel zajistí alokaci finančních prostředků na následující období v rámci provozních nákladů NHS v předpokládané výši uvedené v odstavci 7.3 a). Cena za poskytování podpor výrobce a licencí ve 2. roce (tj. po prvních 12 měsících od akceptace externímu dodavateli IPS sondy) bude fakturována v rámci provozních nákladů služby G5*

6.2. *Objednatel zajistí alokaci finančních prostředků na období od 1. 1. 2026 v rámci provozních nákladů NHS v předpokládané výši uvedené v odstavci 7.3 b) za poskytování podpory externího dodavatele pro zajištění SLA v rámci provozních nákladů služby G5*

7. Prohlášení Poskytovatele

7.1. *Poskytovatel prohlašuje, že příslušné činnosti Poskytovatele (realizované prostřednictvím příslušných pracovních rolí) sloužící k realizaci Plnění dle této Dílčí smlouvy nejsou součástí paušálních plateb generálních ani zákaznických služeb dle čl. 3.2.1 a 3.2.2 Smlouvy o zajištění správy, provozu a rozvoje komunikační infrastruktury, č.j. MV-126064 /SIK5-2018 (dále také „NHS“) ani nejsou v jejich rámci hrazeny. Poskytovatel zaznamená činnosti provedené Plnění dle této Dílčí smlouvy do příslušného interního systému na vykazování činností AVYK.*

7.2. *Realizace Předmětu Dílčí smlouvy nemá bezprostřední dopad do provozní činnosti Objednatele.*

7.3. *Realizace Předmětu Dílčí smlouvy má dopad na provozní náklady Objednatele za:*

a) *Podporu a pořízení licencí pořízených komponent na další období (6 měsíců) ve výši 1 915 000 Kč bez DPH, které budou promítnuty v příslušné kapitole Přílohy 7 NHS. Tyto náklady se projeví u IPS/IDS sond po prvním roce od podpisu předávacího protokolu externímu dodavateli IPS. Tyto náklady se projeví po prvním roce od podpisu předávacího protokolu externímu dodavateli v rámci služby G5.*

b) *Odborné konzultace specialitů IPS k pořízeným komponentám dodavatelem v maximálním množství 300 MD a maximální celkové výši 4 770 000,00 Kč bez DPH. Tyto náklady se projeví následujícím kalendářním roce po podpisu smlouvy a budou fakturovány dle skutečného čerpání v rámci služby G5.*

8. Úprava přechodu vlastnického práva

8.1. *Od data převzetí Plnění na základě akceptačního protokolu dochází k převodu vlastnického práva, resp. práva hospodařit, a postoupení oprávnění k výkonu práva užít Plnění na Objednatele.*

8.2. *Každá ze Smluvních stran nese své náklady spojené s přejímacím řízením sama.*

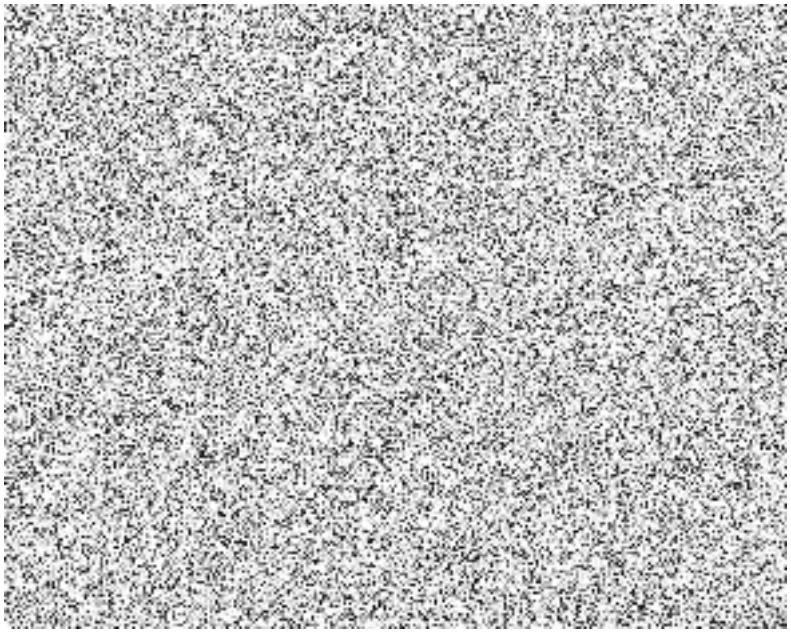
9. Sankce

9.1. Sankce spojené s realizací Plnění jsou upraveny v čl. 16. Rámcové dohody.

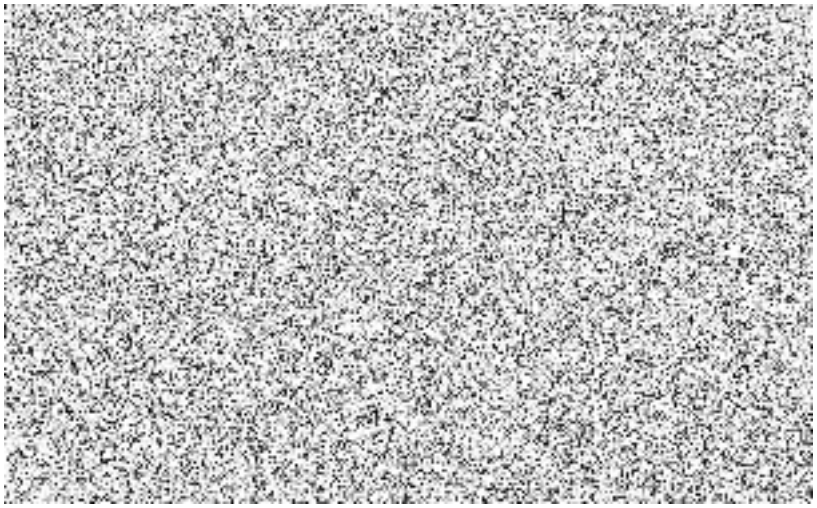
9.2. Pro vyloučení pochybností (s ohledem na čl. 16.1 Rámcové dohody) se uvádí, že pokud je Poskytovatel v prodlení s poskytnutím jen části Plnění dle Dílčí smlouvy je Objednatel oprávněn po Prodávajícím požadovat uhrazení smluvní pokuty ve výši 0,05 % z ceny části Plnění dle Dílčí smlouvy, s jejíž dodáním je v prodlení, a to za každý i započatý den prodlení.

10. Kontaktní osoby

10.1. Kontaktní osoby Poskytovatele



10.2. Kontaktní osoby Objednatele



11. Zpracování osobních údajů

11.1. Pro řádné poskytování Služeb dle této Smlouvy se vyžaduje zpracování osobních údajů zaměstnanců Objednatele a Poskytovatele, jakožto kontaktních osob. Tyto osobní údaje zaměstnanců budou zpracovávány v následujícím rozsahu:

- *jméno a příjmení, titul;*
- *telefonní číslo;*
- *e-mailová adresa.*

11.2. Vznikne-li v průběhu smlouvy nutnost zpracování jiných osobních údajů než kontaktních osob, zavazují se obě smluvní strany k neprodlenému uzavření Zpracovatelské smlouvy v souladu s požadavky Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 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), která se stane nedílnou součástí této smlouvy.

11.3. Zpracování osobních údajů je definováno příslušnou právní úpravou, přičemž se jedná zejména o jejich shromažďování, ukládání na nosiče informací, používání, třídění nebo kombinování, blokování a likvidace s využitím manuálních a automatizovaných prostředků v rozsahu nezbytném pro zajištění řádného poskytování Služeb dle této Smlouvy.

11.4. Osobní údaje budou zpracovávány po dobu poskytování Služeb dle této Smlouvy. Ukončením této Smlouvy nezanikají povinnosti Poskytovatele týkající se bezpečnosti a ochrany osobních údajů až do okamžiku jejich protokolární úplné likvidace či protokolárního předání jinému zpracovateli.

12. Závěrečná ustanovení

12.1. Veškerá ujednání této Dílčí smlouvy navazují na Rámcovou dohodu a touto Rámcovou dohodou se řídí, tj. práva, povinnosti či skutečnosti neupravené v Dílčí smlouvě se řídí ustanoveními Rámcové dohody. V případě, že ujednání obsažené v této Dílčí smlouvě se bude odchylovat od ustanovení obsaženého v Rámcové dohodě, má ujednání obsažené v této Dílčí smlouvě přednost před ustanovením obsaženým v Rámcové dohodě, ovšem pouze ohledně plnění sjednaného v této Dílčí smlouvě. V otázkách touto Dílčí smlouvou neupravených se použijí ustanovení Rámcové dohody.

12.2. Objednatel a Poskytovatel se dohodli, že veškeré Plnění související a poskytnuté v souladu s touto Dílčí smlouvou a Rámcovou dohodou do nabytí účinnosti této Dílčí smlouvy se považuje za Plnění

poskytnuté v souladu s požadavky a podmínkami stanovenými touto Dílčí smlouvou a Rámcovou dohodou a bude tak na něj nahlíženo.

12.3. *Tato Dílčí smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Zveřejněné Dílčí smlouvy v registru smluv zajistí Objednatel.*

12.4. *Smluvní strany prohlašují, že si tuto Dílčí smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.*

12.5. *Pokud v této Dílčí smlouvě není uvedeno jinak, platí ustanovení Rámcové dohody.*

12.6. *Nedílnou Součástí této Dílčí smlouvy je příloha č. 1 – Specifikace předmětu plnění.*

Příloha č. 1 Dílčí smlouvy – Specifikace předmětu plnění

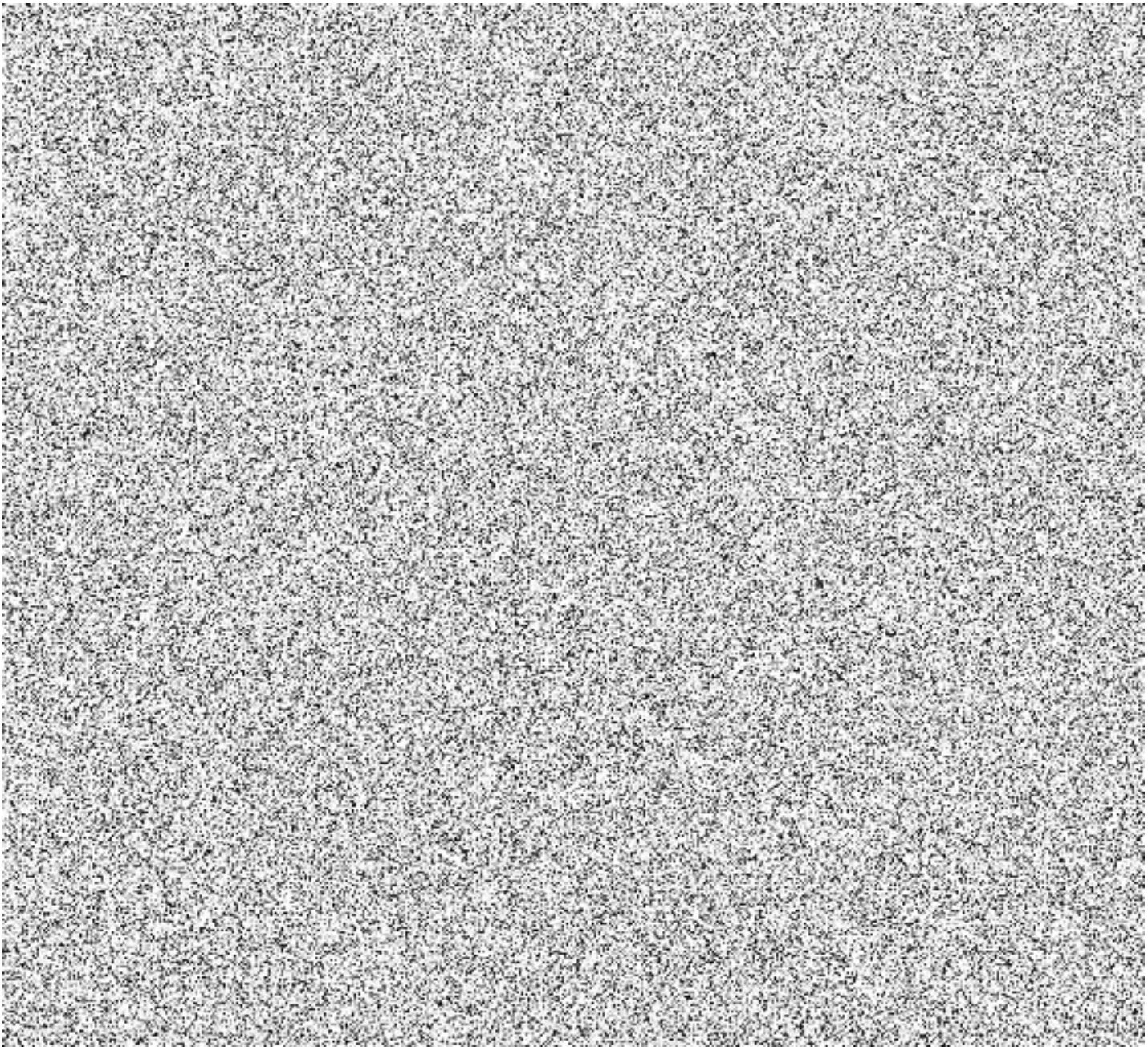
1. Popis současného stavu

1.1. Technologie Trellix (McAfee) IPS v CMS 2.0

Nástroj Trellix (dříve McAfee) Intrusion Prevention System (dále jen „IPS“) funguje jako IDS detekční nástroj (Intrusion detection system) a byl původně zamýšlen jako „anti-DDoS“ řešení pro CMS 2.0.

V případě výpadku IPS sond technologie Trellix (McAfee) dojde k výpadku veškeré internetové konektivity CMS 2.0 – tím také dojde k nedostupnosti veškerých poskytovaných služeb CMS 2.0 s vazbou do veřejné sítě Internet.

Sondy fungují v režimu Active/Stand-by, kdy na aktivní sondě dochází k vyhodnocování jednotlivých bezpečnostních alertů a změnám konfigurace. Následně dochází k synchronizování jednotlivých konfigurací mezi sondami. Proto je důležité práce nejdříve provádět na sondě v režimu Stand-by, aby se zamezilo možnému výpadku konektivity CMS, která momentálně teče přes sondu v Active režimu.



1.2. Technologie Trellix (McAfee) IPS v CMS 2.0

Lokalita	Zařízení	Označení	Sériové číslo	Umístění v DC	Označení racku	Pozice v racku	Typ zapojení	Počet SFP konektorů	Datum ukončení životnosti produktu a podpory od dodavatele
DC Malešice DC1	Trellix IPS NS9100	DC1DD01	J072434084	2-3	F2 3.9	23-24	SFP – 10 GE – MM		30.06.2025
DC Malešice DC1	Trellix IPS NS9100 (Záložní)	DC1DD01-SPARE	J072436035	2-3	F2 3.9	31-32	SFP – 10 GE – MM		30.06.2025
NDC Vápenka DC2	Trellix IPS NS9100	DC2DD01	J072442018	301	MVP6	27-28	SFP – 10 GE – MM	8	30.06.2025

Tabulka 1 - Seznam zařízení IPS Trellix v CMS 2.0

2. Návrh technického řešení

Detailní technický návrh řešení (TNŘ) - bude zpracován až po vyhlášení vítěze v rámci VZ na výměnu technologie IPS pro CMS2.0.

Realizace technického řešení bude prováděna za účasti provozních týmů CMS (datové sítě, infrastruktura), a to včetně zajištění odborného předání ze strany realizátora.

Navrhované řešení IPS je náhradou provozovaného technologie IPS-NS9100 od výrobce Trellix, v celkovém počtu 3ks IPS hardwarové sond (2ks aktivní a 1ks náhradní), technologie je on-premise ve dvou geograficky oddělených datových centrech, ve dvou lokalitách.

Celá správa IPS bude řešena on-premise. Jakékoliv cloudové řešení není přípustné.

Pořízené řešení IPS bude používat minimálně metodu signaturové detekce s pravidelnými aktualizacemi a možnost vytváření a importování vlastních signatur.

Řešení IPS bude schopné provádět úpravu generování jednotlivých alertů za pomocí uživatelsky definovaných politik, nebo pomocí tzv. „Whitelistování“.

Řešení IPS bude schopné pracovat se síťovým provozem za pomocí protokolů ISO/OSI vrstvy č.3 - IPv4 a IPv6, a také schopné provádět operace IPS až do úrovní protokolů ISO/OSI vrstvy č.7.

IPS bude umět provádět úpravu síťového provozu, například pomocí blokování GeoIP nebo jednotlivých síťových subnetů a detekci na základě prahových hodnot a heuristické analýzy.

IPS bude schopno provádět překlad síťové komunikace ze dvou navzájem nezávislých virtuálních lokálních sítí (VLAN) – tzv. „VLAN-Translace

Řešení IPS, a jednotlivé komponenty, bude spravováno centrálně včetně pokročilé správy, jako například aktualizování databáze signatur a vytváření záloh jednotlivých komponent.

Celé řešení bude připojeno do monitorovacího a dohledového nástroje Zabbix, a to pomocí monitorovacích agentů, nebo SNMP verze 3 protokolu.

IPS bude zaznamenávat a předávat bezpečnostní a provozní události dle požadavků zákona č. 181/2014 Sb. (dále jen „ZoKB“) ve znění pozdějších předpisů, do SIEM řešení pomocí protokolu Syslog, kde preferovanou variantou je využití CEF standartu

Fyzický hardware / hardwarová appliance výrobce s instalací do datového rozvaděče

2.1. Pořizovaná technologie

Druh komponenty	Popis komponenty	Počet
IPS/IDS sonda	*Trellix Network Security IPS NS9600 Appliance v uvedeném celkovém počtu 3ks IPS sond jsou 2ks aktivní a 1ks náhradní.* *Trellix Network Security 8-Port 10/1 GigE SR Fiber Network I/O Expansion Module (with Built-In Fail-Open) vždy po 1ks per aktivní IPS*	*3*
Licence	*Trellix Network Security IPS NS9600 Appliance - Advanced RMA (next business day ship) Hardware Support* *Trellix IPS NS9600 - 20Gbps Software license (Throughput based entitlement) - subscription licence* *Trellix IPS NS9600 - 20Gbps Failover (HA) Software license (Throughput based entitlement) - subscription licence* *Trellix Network Security 8-Port 10/1 GigE SR Fiber Network I/O Expansion Module (with Built-In Fail-Open) - Advanced RMA (next business day ship) Hardware Support* *Trellix Network Security Manager Software Subscription Standard Edition - subscription licence*	*3*
Podpora	*Servisní podpora a Service-level agreement na 1. rok*	*3*

2.2. Technické specifikace IPS sond

Id	*Požadavek*	*Hodnota*
1.	**Funkční požadavky**	
1.1.	Fyzický hardware / hardwarová appliance výrobce s instalací do datového rozvaděče	ANO
1.2.	Provoz ve vysoké dostupnosti mezi datovými centry	ANO
1.3.	Možnost budoucí škálovatelnosti až na hranici provozu 300 Gbps (6x100GBps) v režimu vysoké dostupnosti.	ANO
1.4.	Funkce IDS	ANO
1.5.	Funkce IPS	ANO
1.6.	Detekce síťových protokolů až na úroveň ISO/OSI vrstvy č.7 v reálném čase	ANO
1.7.	Blokace síťových protokolů až na úroveň ISO/OSI vrstvy č.7 dle uživatelsky definovaných pravidel v reálném čase	minimálně 5,000
1.8.	Počet DDoS profilů	minimálně 30,000
1.9.	Počet ACL pravidel	ANO
1.10.	Provoz v tzv. „ostrovním režimu“ bez dostupnosti internetu	ANO
1.11.	Možnost nastavení více úrovňové oprávnění (RBAC)	ANO
1.12.	Ověřování vůči interním doménám (například pomocí RADIUS nebo LDAP)	ANO
1.13.	Manuální odchytávání síťové komunikace (PCAP)	ANO
1.14.	Možnost škálování IPS sond řešení pro zvýšení propustnosti	ANO

Id	Požadavek	Hodnota
1.15.	Překlad virtuálních lokálních adres (VLAN translace)	ANO
1.16.	Možnost nastavení průchodu provozu bez VLAN translace (Passthru)	ANO
1.17.	Zálohování jednotlivých komponent přes společnou správu IPS	ANO
1.18.	Technologie může být použitá, nesmí být kompromitována či poškozená (ručí dodavatel).	
1.19.	Podpora ze strany výrobce musí být po celou dobu požadovaného životního cyklu řešení – 5let od zahájení řízení veřejné zakázky, tj. nesmí vyjít po tuto dobu z podpory.	
2.	**Bezpečnostní požadavky**	
2.1.	Technologie musí reflektovat varování NÚKIB z hlediska hrozeb a ekonomickým sankcemi - Ruská federace a Bělorusko, Huawei a ZTE.	ANO
2.2.	Technologie musí splňovat požadavky zákona č. 181/2014 Sb. „Zákon o kybernetické bezpečnosti“ a dalších navazujících předpisů.	ANO
3.	**Rozšířená detekce hrozeb**	
3.1.	Protokolová příchozí dekrypce síťového provozu SSL/TLS bez dopadu na výkon dané IPS sondy	ANO
3.2.	Odchozí SSL/TLS dekrypce síťového provozu	ANO
3.3.	Řešení musí umožnit dekrypci kryptografických algoritmů dle aktuálního NÚKIB „Doporučení v oblasti kryptografických prostředků“ viz: https://nukib.gov.cz/download/publikace/podpurne_materialy/Minimalni_pozadavky_v4_FINAL.pdf https://nukib.gov.cz/download/publikace/podpurne_materialy/Minimalni_pozadavky_Priloha_v2_FINAL.pdf	ANO
3.4.	Podporované SSLv3 kryptografické algoritmy: TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_SEED_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_NULL_SHA TLS_RSA_WITH_NULL_MD5 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_DH_anon_WITH_AES_256_CBC_SHA TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_SEED_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_SEED_CBC_SHA TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA TLS_DH_anon_WITH_RC4_128_MD5 SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	ANO
3.5.	Podporované SSL TLS verze 1.2 kryptografické algoritmy: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ANO

Id	Požadavek	Hodnota
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_256_CCM_8 TLS_RSA_WITH_AES_256_CCM TLS_RSA_WITH_ARIA_256_GCM_SHA384 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_128_CCM_8 TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_ARIA_128_GCM_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_RSA_WITH_NULL_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_DHE_RSA_WITH_AES_256_CCM_8 TLS_DHE_RSA_WITH_AES_256_CCM TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 TLS_DH_anon_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 TLS_DH_anon_WITH_AES_256_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_CCM_8 TLS_DHE_RSA_WITH_AES_128_CCM TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 TLS_DH_anon_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_DH_anon_WITH_AES_128_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	

Id	Požadavek	Hodnota
3.6.	Podporované SSL TLS verze 1.3 kryptografické algoritmy: TLS_AES_128_CCM_SHA256 TLS_AES_128_CCM_8_SHA256 TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256	ANO
4.	**Funkce IPS/IDS**	
4.1.	Definování uživatelsky definovaných signatur jako doplnění signatur definovaných výrobcem	ANO
4.2.	Nativní podpora pro SNORT signatury	ANO
4.3.	Blokování v reálném čase na základě kombinování behaviorální analýzy a signaturové detekce	ANO
4.4.	Úprava generovaných alertů za pomocí definovaných politik (např. Whitelisting)	ANO
4.5.	Automatické přepínání v případě failover stavu a následná funkce failback	ANO
5.	**Detekce a ochrana botnetů a malware**	
5.1.	Detekce a blokace Botnetů a Malware	ANO
5.2.	Detekce a blokace C2C	ANO
5.3.	Definování uživatelsky definovaných signatur jako doplnění signatur definovaných výrobcem	ANO
5.4.	Korelace nad více útoky	ANO
6.	**DoS a DDoS ochrana**	
6.1.	Detekce na základě prahových hodnot a heuristické analýzy	ANO
6.2.	Vlastní učení na základě probíhajícího provozu	ANO
6.3.	Ochrana na základě uživatelsky definovaných profilů	
6.4.	Limitace počtu spojení na jednotlivé hosty	ANO
6.5.	Možnost blokování na základě uživatelsky definovaných IP nebo GeIP databáze aktualizované výrobcem	
7.	**Management**	
7.1.	Správa zařízení přes webový management HTTPS	ANO
7.2.	Správa zařízení přes příkazovou řádku CLI – protokol SSH	
7.3.	Správa přes konzolový port RS232 – RJ-45 zásuvka	ANO
7.4.	Dedikovaný port pro správu 1GbE	ANO
7.5.	SNMPv3	ANO
7.6.	Management aplikace či VM appliance pro společnou správu všech instalovaných sond pro každé datové centrum	ANO
7.7.	Management aplikace či VM appliance musejí umožnit fungování v režimu multi-master	ANO
8.	**Monitoring**	
8.1.	Sběr událostí ohledně přihlášení a uživatelských akcí ve správě IPS	ANO
8.2.	Zasílání logů protokolem Syslog dle specifikací IETF/RFC 5424, nebo IETF/RFC 5425(TLS) pro splnění požadavků ZoKB	ANO
8.3.	Monitoring pomocí monitorovací technologie pomocí monitorovacích agentů nebo SMTP verze 3 protokolu (například Zabbix)	ANO
9.	**Požadovaný výkon jedné IPS sondy**	

Id	*Požadavek*	*Hodnota*
9.1.	Požadovaný agregovaný výkon	minimálně 20Gbps
9.2.	Maximální agregovaný výkon – možnost navýšení až na	minimálně 60Gbps
9.3.	Maximální propustnost (UDP, 1512B)	15 Gbps
9.4.	Nová připojení za sekundu	450 000
9.5.	HTTP připojení za sekundu	260 000
9.6.	Propustnost při dešifrování SSL	minimálně 10Gbps
9.7.	Maximální počet SSL toků	1 000 000
9.8.	Počet importovaných SSL klíčů	1 024
9.9.	Počet virtuálních IPS systémů	1 000
9.10.	Maximální počet DoS profilů	5 000
9.11.	ACL pravidla	minimálně 10 000
10.	**Síťové komunikační porty**	
10.1.	10/1 Gb Ethernet porty včetně SFP+ - Multi-Mode	Minimálně 6 ks
10.2.	Zabudované porty 100 Gb Ethernet porty	Minimálně 4ks
10.3.	Možnost rozšíření na 100 Gb Ethernet porty	Minimálně 12ks
10.4.	Dedikovaný Out-Of-Band management port 1GbE BASE-T (metalický port R45)	1ks
10.5.	Dedikovaný konzolový port RS232 se zásuvka RS45	ANO
11.	**Fyzické vlastnosti IPS sondy**	
11.1.	Interní úložiště redundantní	400 GB M.2 NVMe disk
11.2.	Zařízení musí obsahovat redundantní zdroje napájení 240V/50Hz s napájecími kabely C13/C14	ANO
11.3.	K veškerému dodávanému HW musí být předáno Prohlášení o shodě.	ANO
11.4.	Chlazení v režimu teplé/studené uličky	Předo-zadní/ zado-přední
12.	**Rozměry**	
12.1.	Montáž do racku 19“	ANO
12.2.	Maximální hloubka pro montáž do racku 80 cm	ANO

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.

Vstupující dokument byl podepsán zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru a platnost zaručeného elektronického podpisu byla ověřena dne 01.12.2025 18:46:01.

Zaručený elektronický podpis byl shledán platným, dokument nebyl změněn a ověření platnosti kvalifikovaného certifikátu bylo provedeno vůči seznamu zneplatněných kvalifikovaných certifikátů k datu 01.12.2025 10:56:12. Údaje o zaručeném elektronickém podpisu: číslo kvalifikovaného certifikátu 016A8254, kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru PostSignum Qualified CA 4, Česká pošta, s.p. pro podepisující osobu Jan Ďoubal, Národní agentura pro komunikační a informační technologie, s. p.. Elektronický podpis nebyl označen platným časovým razítkem.

Typ vstupního dokumentu:	.PDF
Otisk souboru:	13B5532D16A1676BC1A0F2CBF90F9F5830B064A301E1EFFA669E5D50E457F51A
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:

Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:

1.12.2025

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:

Horáčková Jana

Elektronický podpis: 2.12.2025
Certifikát autora podpisu:
Jméno: Mgr. Roman Nový
Vydal: NCA SubCA1/RSA 10/2023
Platnost do: 8.1.2028 15:11 +01:00

Elektronická pečeť - 1.12.2025
Certifikát :
Jméno : MVCR - pečeť spisové služby