Příloha č. 1: Technická specifikace

Technickými podmínkami se v případě plnění této Smlouvy rozumí vymezení charakteristik a požadavků na plnění předmětu veřejné zakázky. Při výkladu technických podmínek je vždy nutné přihlížet k účelu využití předmětu veřejné zakázky pro odběratele.

Pokud stanovené technické podmínky, obsahují požadavky nebo odkazy na názvy či specifická označení dodávek, která platí pro určitou osobu za příznačné, jedná se výhradně o případy, kdy by popis předmětu veřejné zakázky postupem podle § 89 a násl. ZZVZ nebyl dostatečně přesný, jednoznačný a srozumitelný. **Odběratel však umožní pro plnění Smlouvy použití i jiných, kvalitativně a technicky obdobných řešení.**

[DOPLNÍ DODAVATEL PODLE SVÉ NABÍDKY PODANÉ DO VEŘEJNÉ ZAKÁZKY]

Příloha č. 1: Technická specifikace

Obsah

1. Popis navrhovaného aplikačního řešení

Předmětem této veřejné zakázky je dodávka **vybraných prvků demonstrativní aplikace** ekosystému sítí 5G, v podobě uceleného technologického ekosystému zahrnující, mimo jiné, zajištění 5G konektivity, modernizaci vybavení klíčových strategických a zájmových bodů městské infrastruktury, rozvoj kyberbezpečnosti v oblasti datové sítě města skrze síťovou sondu včetně navazujícího vybavení a implementace monitoringu provozu koncových bodů na území města.

Cílem zadavatele je vybudovat **Metropolitní datovou síť** Ústí nad Labem, která bude disponovat nejvyššími standardy kybernetické bezpečnosti s konektivitou 5G sítě.

V rámci řešení budou zajištěny všechny klíčové výstupy, tak jak je definoval zadavatel:

- Nasazení technologie 5G resp. zvýšení využití sítě 5G
- Zvýšení ochrany a dostupnosti koncových bodů klíčové strategické infrastruktury (dále jen KI) a zájmových bodů města
- Zavedení opatření pro ochranu API v rámci 5G sítě (autentizace a autorizace, šifrování dat, monitorování provozu pro identifikaci neobvyklých aktivit/potenciálních hrozeb, automatizované učení pro automatickou reakci bezpečnostního systému na hrozby)
- Nasazení nástrojů pro analýzu síťového provozu, monitorování sítě a vyhodnocování událostí, systémy detekce a prevence proniknutí do sítě
- Zavedení síťové sondy pro hlídání anomálií v technologickém procesu komunikace vnitřní sítě s využitím síťové sondy
- Navýšení kapacit k ochraně sítě
- Monitorování vzdálených přípojných míst

Adresy koncových bodů KI a zájmových bodů města:

Rozvodna Výstupní MR11 - ZOO
Rozvodna MR 2 – V Podhájí
Rozvodna MR 3 – Kočkovská
Rozvodna MR 4 – Majakovského
Rozvodna MR 5 – Jungmanova
Rozvodna MR 6 – Všebořická
Rozvodna MR 7 – Seifertova
Rozvodna MR 8 – Děčínská
Rozvodna MR 9 - Nová
Rozvodna MR 10 – Karla IV.
Rozvodna a dispečink Bratislavská
Převaděč VISO – DPS Vyhlídka
Převaděč VISO – ZŠ a MŠ Jitřní
Mateřská škola Vaňov
Mateřská škola Svádov
PB Centrum (sídlo Metropolnet)*

* v době realizace projektu probíhá celková rekonstrukce objektu Na Předmostí. Router bude krátkodobě instalován v prostorách PB Centra, sídla městské akciové společnosti Metropolnet, a.s. Po dokončení rekonstrukce bude router a na něj vázaná 5G konektivita přesunuta do zrekonstruovaného objektu Na Předmostí.

1.1 Operátorská konektivita – Eliminace SPOF u předávacího bodu operátora

Požadavky zadavatele:

Zadavatel uvedl, že v rámci stávajícího technického propojení 5G sítě a metropolitní sítě jsou koncová zařízení v 5G síti připojena k privátní APN s interním neveřejným IP adresním prostorem. Předávacím rozhraním mezi infrastrukturou operátora 5G a interní datovou infrastrukturou Metropolnet, a.s. je 1Gbit Ethernet mezi routery poskytovatele sítě 5G a metropolitní sítí v jednom datovém uzlu.

Za účelem zvýšení dostupnosti 5G neveřejné datové infrastruktury plánuje zadavatel vytvořit druhý propojovací bod interní infrastruktury metropolitní sítě s operátorem 5G v některém z datových uzlů správce sítě.

Zadavatel požaduje vytvoření redundantní konektivity v ul. Hoření 13 ke stávajícímu propojovacímu místu mezi 5G infrastrukturou poskytovatele datových služeb a optickou sítí Metropolnet, a.s.

Nová, redundantní konektivita má být vytvořena v objektu Městské policie Ústí nad Labem, Na Nivách 1800/27, v prostorách serverovny (místnost 3.07) operačního střediska městské policie v racku č.3.

Zadavatel uvedl že pro připojení optického kabelu je možné využít stávající vybudovanou trasu z kabelové komory na pozemku objektu vedle plotu a chodníku ulice U Jeslí (orientační umístění komory viz schéma) a pro zavedení optického kabelu je možné poskytnout mikrotrubičku 10/8, která vede z kabelové komory k racku do místnosti 3.07.

Požadavek zadavatele	Nabízené řešení splňuje (ano/ne)	Poznámka
Zařízení pro redundantní konektivitu musí umožnit montáž do racku, nebo společně se zařízením musí být dodaná police pro rack 19“, hloubka racku je 100 cm.	ano	
Pro využití mikrotrubičky je nutná koordinace se správcem infrastruktury Metropolnet, a.s.	ano	
Mechanismy a principy přepojování primární/záložní konektivity musí být koordinovány se správcem optické infrastruktury Metropolnet, a.s.	ano	
Fyzická konektivita • Typ rozhraní: Optické SFP/SFP+ / SFP transceiver 1Gbit RJ45. • Rychlost připojení: 1 Gbps nebo 10 Gbps (podle požadavků a dostupné infrastruktury). • Požadavky na kabeláž: CAT6 pro metalické vedení nebo LC konektory pro optiku.	ano	Rychlost připojení: 1 Gbps

Podpora VLAN • Pro Layer 2 komunikaci: Transparentní přenos provozu mezi LAN zákazníka a poskytovatele prostřednictvím dedikované VLAN. • Možnost trunk konfigurace: IEEE 802.1Q (dot1q) tagging pro podporu více VLAN na jednom fyzickém portu. • Možnost nativní VLAN: Pouze po dohodě	ano	
Podpora Layer 3 (L3) routingu • IP adresy: Dedikované podsítě pro komunikaci mezi interní LAN zadavatele a poskytovatele služby. • IP podsíť: Zadavatel přidělí adresní IP rozsahy podsítí poskytovatele služby. • Routing protokoly: Statické trasy nebo dynamické routing protokoly (např. OSPF, BGP) dle dohody. • NAT (Částečně volitelné): Možnost provádění NAT na straně poskytovatele nebo zákazníka dle potřeby.	ano	
Bezpečnost • Access Control Lists (ACL): Na straně poskytovatele služby pro omezení přístupu podle pravidel.	ano	
SLA (Service Level Agreement) • Dostupnost: 99,5% nebo vyšší podle dohody. • Latence: Max. 10 ms výměna mezi připojenými LAN segmenty (pro lokální propojení). • Podpora: 24/7 technická podpora a eskalační plán pro řešení incidentů.	ano	Eskalační plán pro řešení incidentů bude vytvořen a oboustranně odsouhlasen před podpisem Smlouvy o dílo.

1.2 Modernizace vybavení klíčových bodů městské infrastruktury

Požadavky zadavatele:

Zadavatel počítá s nákupem **5G pokročilých průmyslových modemů**. K pořízeným 5G modemům mají být do řešených míst měníren paralelně instalovány a připojeny **bezpečnostní senzory** za účelem zvýšení fyzické bezpečnosti u strategických infrastrukturních objektů.

Senzory budou napojeny na operační středisko městské policie a monitorovací notifikační systém. V rámci senzorů bude zároveň nastavena funkce detekce osoby (prostřednictvím analytiky), pro zajištění automatizovaného hlášení přítomnosti osob v chráněném zorném poli.

Rozvaděč kamery s 5G routerem má být vždy instalován v měnírnách, kamery mají být instalovány přímo na fasádě rozvodny, případně na (poptávaném) výložníku, podle místní dispozice. Přenos signálu a napájení od routeru ke kamerám má být řešeno jedním kabelem (PoE) v trubkách.

Seznam bodů KI (měnírny, rozvodny), kde budou instalovány detektory – pevné kamery:

Rozvodna MR 2 – V Podhájí

Rozvodna MR 4 – Majakovského

Rozvodna MR 5 – Jungmanova

Rozvodna MR 6 – Všebořická

Rozvodna MR 7 – Seifertova

Rozvodna MR 8 – Děčínská

Rozvodna MR 9 - Nová

Rozvodna MR 10 – Karla IV.

Požadavek zadavatele	Nabízené řešení splňuje (ano/ne)	Poznámka
Minimální technické požadavky na detektory – pevné kamery:		
Rozlišení min. 5 MPx při 30 pps	ano	
Ohnisková vzdálenost objektivu 2,7 – 12 mm / F 1,2	ano	F 1,0
Automatická clona a ostření	ano	
Citlivost snímače min. 0,05 Lux (barevně) a 0 Lux při použití přísvitu (černobíle)	ano	
Hardwarová podpora IR přísvitu pomocí mechanického filtru, automatické přepínání režimů den/noc	ano	Kamera vybavená funkcí FULL COLOR
Zabudovaný řízený IR přísvit, dosvit min. 50 m	ano	
Komprese H.265/H.264/MJPEG	ano	
Podpora „chytrých“ (Smart) kodeků pro video za účelem snížení přenášených a ukládaných dat	ano	
Minimálně 3 nezávislé video streamy s různým nastavením současně v režimu Unicast	ano	
Kompenzace protisvětla, WDR min. 120 dB	ano	
Stabilizace obrazu	ano	

Redukce šumu	ano	
Rozhraní RJ-45 (10/100BASE-T)	ano	
Přenos dat šifrovaný pomocí HTTPS, ověřování přihlášení metodou Digest	ano	
Stupeň krytí min. IP66	ano	IP67
Antivandal provedení úrovně min. IK10	ano	
Napájení kamery pomocí PoE, respektive PoE+, PoE++ či midspan pro plynulý provoz kamery	ano	
Provozní teplota min. -40° až +55° C	ano	
Zajištění plné komunikace kamery a stávajícího SW Geutebrück	ano	
filtrování IP adres, protokol uživatelských přístupů, ověřování pomocí 802.1x	ano	
Montáž kamery na fasádu objektu nebo na konzoli na fasádě objektu, na ocelovém sloupu	ano	
Záruka v délce 60 měsíců	ano	
Účastníkem nabízený výrobek (identifikujte výrobce, název a typové označení výrobku)	ano	Název a typové označení: Pevná kamera Dahua IPC-HFW3549T1-ZAS-PV-27135-S5 Výrobce: Zhejiang Dahua Technology Co., Ltd
Součástí dodávky musí být potřebné výložníky	ano	
Data z kamerových bodů budou přenášena prostřednictvím signálu 5G.	ano	
Kamerový rozvaděč bude součástí této dodávky a stavby	ano	
Umístění kamerových bodů bude na fasádě objektu, případně na stávajících ocelových stožárech	ano	
Licence:		
Součástí dodávky bude 8 licencí pro připojení kamer do provozovaného VMS Geutebrück: ○ Geutebrück licence řady G-Core/SIM	ano	
Rozvaděče Dodávka musí zahrnovat rozvaděče a další potřebné vybavení pro provoz 8 kamer, min.:		

Podružný jistič	ano	
Proudový chránič	ano	
Přepěťovou ochranu	ano	
DIN lištu pro montáž 5G routeru a dalších prvků	ano	
Kabelové průchodky	ano	
Řešení kamerových bodů a rozvaděčů musí zahrnovat veškeré potřebné další materiály (úchyty, kabeláž, montážní prvky) vyplývající z dodávaného řešení. Veškeré komponenty musí respektovat a naplňovat standardní zákonné a normativní požadavky (např. elektroinstalace).	ano	

Budou dodány **pevné kamery IPC-HFW3549T1-ZAS-PV-27135-S5**, produktový list předložil dodavatel ve své nabídce.

1.3 Síťová sonda – dodávka, integrace, licence

Bude dodán Systém pro analýzu síťového provozu a bezpečnostní monitoring, který identifikuje bezpečnostní rizika a události a splňuje klíčové požadavky zadavatele, jak je uvedeno níže.

1.3.1 Dodávka a integrace síťové sondy

Bude dodáno řešení **FortiNDR™ On Premise Solution** od firmy Fortinet, prostřednictvím poddodavatele Exclusive Networks Czechia s. r. o.. Produktový list předložil dodavatel ve své nabídce.

Obecné informace			
Požadované informace		Výrobce / verze / part number	
Seznam a popis nabízeného řešení – výrobce / verze / part number.		**Fortinet / FortiNDR 100F / FNR-1000F** **Fortinet / FortiAnalyzer-VM Subscription License with Support - 10GB / FC1-10-AZVMS-465-01-60**	
Obecné požadavky			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_01_01	Systém musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a	ano	FortiNDR analyzuje provoz v reálném čase, detekuje anomálie a kybernetické

	anomální chování a musí o nich v reálném čase vytvářet upozornění.		hrozby pomocí AI/ML modelů a generuje alerty.
POŽ_1_01_02	Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	ano	FortiNDR pracuje s pasivním zrcadleným provozem (SPAN/TAP) a nevyžaduje žádné agenty.
POŽ_1_01_03	Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection) do L7 (dle ISO/OSI), nikoli pouze čísla portu (L4 dle ISO/OSI).	ano	Používá DPI a aplikační detekci do úrovně L7 (protokol, aplikace) dle OSI.
POŽ_1_01_04	Systém musí být plně funkční v on-premise prostředí Zadavatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	ano	Celý systém je plně provozuschopný v on-premise bez jakéhokoliv cloudového propojení, vyjma komunikace na cloud výrobce pro stahování nových signaturních detekcí.
POŽ_1_01_05	Aktualizace systému musí být možné provádět z uživatelského prostředí systému.	ano	Uživatelské rozhraní umožňuje kontrolu a provedení aktualizací.
Požadavky na ukládání síťových toků			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_02_01	Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	ano	FortiNDR ukládá sítě toků a metadata L2-L7, včetně aplikačních transakcí.
POŽ_1_02_02	Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, IRC, SSH, LDAP, LDAPS, KERBEROS, SNMP, RTPS, RP, CIFS, MYSQL, MSSQL,POSTGRESQL, RDP, SIP, FTP, FTP-DATA, TFTP-DATA, SSL/TLS zapouzdření a možnosti podpory OT/SCADA protokolů DNP3, MODBUS, IEC104, ETHERNET_IP, PROFINET, BACNet	ano	Plná podpora protokolů: DNS, SMB, HTTP(S), SMTP(S), POP3, IMAP, SSH, LDAP(S), KERBEROS, SNMP, CIFS, DB protokoly, OT/SCADA.
POŽ_1_02_03	Je požadováno uchování historie datových toků na dobu minimálně 2 měsíců.	ano	Dodávaný systém je škálován pro datovou retenci minimálně 2 měsíců.

Požadavky na analýzu a sběr aplikačních a systémových logů			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_03_01	Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity nebo umožnit export, sběr a analýzu uvedených logů do stávajícího logovacího nástroje FortiAnalyzer.	ano	Zpracování logů bude probíhat v nástroji FortiAnalyzer s jehož implementací a nasazením počítáme v předkládané cenové nabídce.
Požadavky na uživatelské rozhraní			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_04_01	Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.	ano	Jednotné GUI pro detekce, alerty, nastavení, dashboardy a reporty.
POŽ_1_04_02	Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně: • granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu; • vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	ano	Systém podporuje RBAC, uživatelských pohledů a granularitních oprávnění.
Požadavky na automatická hlášení (alerty) a reporting			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_05_01	Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu.	ano	Email a log notifikace s filtrováním dle různých parametrů (subnet, země, služby atd.).
POŽ_1_05_02	Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.	ano	Alerty exportovatelné ve strojově čitelném formátu (např. JSON, CEF) s URL odkazy.

Požadavky na integraci			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_06_01	Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně: • syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat); • přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní; • přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní " s integrací do stávajícího logovacího nástroje FortiAnalyzer a možností výstupu do SIEM nástroje, • integrace se službami identity uživatelů (minimálně LDAP) bez nutnosti konfigurace zasílání logů do systému sondy, pro párování detekcí s uživateli.	ano	Podpora syslog, CEF/LEEF, integrace s FortiAnalyzer a LDAP identitou.
POŽ_1_06_02	Integrace volitelně buď pomocí API, nebo proprietárními protokoly s firewally: • Fortinet; • Palo Alto; • Cisco;	ano	Integrace s produkty výrobce Fortinet je zaručena skrze Fortinet Security Fabric. Integrace na ostatní výrobce je pomocí API.
Obecné požadavky na architekturu a případný HW			
POŽ_1_07_01	Možnost nasazení systému jako: • HW appliance (specializovaný HW výrobce), • nasazení na vyhrazeném HW (např. server, server +diskové pole atd.) • SW appliance (do virtualizační platformy VmWare)	ano	Dodávané řešení (NDR +FortiAnalyzer) je možné nasadit jako VM či HW
POŽ_1_07_02	Pro všechny případné HW komponenty je požadován rack-mount 1U nebo 2U zařízení o velikosti 19“. Zadavatel neomezuje počet HW na řešení. Zadavatel bude vyžadovat v nabídce blokové schéma nabízeného řešení.	ano	1U nebo 2U rack-mount. Blokové schéma bude součástí dodávky. Jednoduché blokové schéma – viz obrázek č. 1 níže
POŽ_1_07_03	Pro všechny případné HW komponenty je požadován duální zdroj napájení se schopností hot-swap.	ano	Všechny dodávané HW obsahují redundantní zdroje.

POŽ_1_07_04	Pro všechny HW komponenty řešení je požadováno samostatné síťové rozhraní pro vzdálenou správu.	ano	Ano systémy obsahují remote managment rozhraní
Požadavky na pokrytí IT prostředí			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_08_01	V síti je předpokládáno do 1000 aktivních zařízení s průměrným celkový průtokem do 500 Mbps, řešení musí být na tyto hodnoty dimenzováno. Sběr bude probíhat v jedné lokalitě (monitorovací linka ze core prvku Zadavatele).	ano	Dodávané řešení je dimenzované na požadovaný datový tok.
POŽ_1_08_02	V případě použití HW bude vyžadováno rozhraní na 1 x GE (metalické nebo SFP SM).	ano	Ano systém toto splňuje.
Požadavky na monitorování zařízení, segmentů sítě a využívaných síťových služeb			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_09_01	Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. a zároveň na základě učícího se algoritmu zobrazuje anomálie (odkud se systém připojuje, kam IP/geo lokace, počet přenesených dat, apod.)	ano	Dodávané řešení umožňuje automatickou identifikaci zařízení, geolokaci a dále pak dodávané řešení obsahuje učící algoritmy pro anomálie.
Požadavky na samostatné učení behaviorálních aktivit a detekce anomálií			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_10_01	Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci monitorovaných segmentů.	ano	AI modely chování, detekce odchylek od normy, pokrytí TCP/UDP portů 0-65535 včetně IPv6.
POŽ_1_10_02	Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro: • odchylku od modelu pro přenos dat, toků a paketů; • odchylku od modelu pro počet síťových toků a využitých síťových služeb; • odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	ano	AI modely chování, detekce odchylek od normy, pokrytí TCP/UDP portů 0-65535 včetně IPv6.

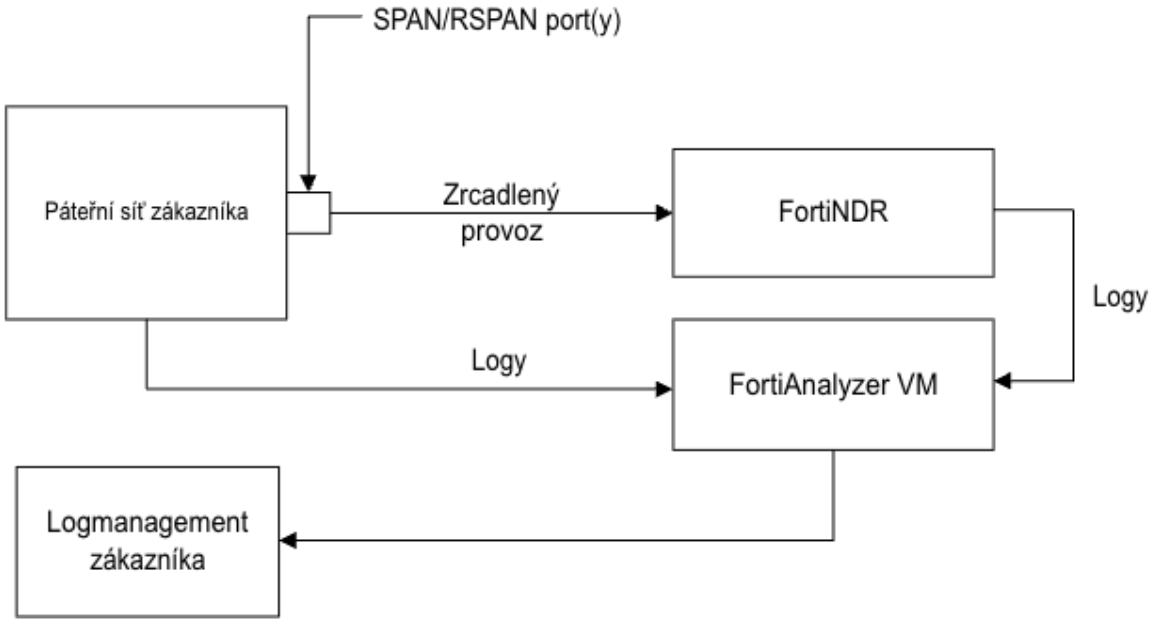
POŽ_1_10_03	Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.	ano	AI modely chování, detekce odchylek od normy, pokrytí TCP/UDP portů 0-65535 včetně IPv6.
Požadavky na detekce na základě databáze známých hrozeb			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_11_01	Systém musí být schopen identifikovat hrozby a reportovat události na základě: • detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel; • reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	ano	Detekce dle signatur, reputační databáze, aktualizace každou hodinu, zobrazování dat z paketů.
POŽ_1_11_02	Databáze zmíněné v požadavku výše musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora.	ano	Detekce dle signatur, reputační databáze, aktualizace každou hodinu, zobrazování dat z paketů.
POŽ_1_11_03	Systém musí využívat tuto detekci pro veškerý monitorovaný provoz, nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.	ano	Detekce dle signatur, reputační databáze, aktualizace každou hodinu, zobrazování dat z paketů.
POŽ_1_11_04	Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, na základě kterých se provádí inspekce veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	ano	Detekce dle signatur, reputační databáze, aktualizace každou hodinu, zobrazování dat z paketů.
POŽ_1_11_05	Systém ukáže uživateli aplikační data přenášená v paketech na základě, kterých bylo učiněno rozhodnutí detekce.	ano	Detekce dle signatur, reputační databáze, aktualizace každou hodinu, zobrazování dat z paketů.
Analýza šifrované komunikace			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_12_01	Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace,	ano	Dodávané řešení umožňuje provádět TLS

	minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.		fingerprinting a detekce škodlivé šifrované komunikace.
Požadavky na asistované učení			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_13_01	Je požadován uživatelsky přívětivý proces práce s definovanými pravidly pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů a jejich kombinace: • IP adresa; • MAC adresa; • hostname; • segment sítě / podsítě; • lokalita – ASN, země, apod.; • směr komunikace – určení klienta, nebo serveru; • detekovaná událost – kategorie, název apod; • použité služby, protokolu, portu; • libovolné kombinaci výše popsaných.	ano	Definice pravidel pro zpřesnění detekce, potlačení false-positives i v historii je v dodávaném řešení implementována.
POŽ_1_13_02	Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	ano	Definice pravidel pro zpřesnění detekce, potlačení false-positives i v historii je v dodávaném řešení implementována.
Požadavky na vyhledávání, filtrování a vizualizaci dat			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_14_01	Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka. Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně: • podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN;	ano	Okamžité filtrování a vizualizace, forenzní analýza bez nutnosti dotazovacího jazyka.

	prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.		
POŽ_1_14_02	Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	ano	Dodávané řešení podporuje zobrazení kontextu zařízení (hostname, OS, MAC, tagy, poznámky, reputace).
POŽ_1_14_03	Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, IRC, SSH, LDAP, LDAPS, KERBEROS, SNMP, RTPS, RP, CIFS, MYSQL, MSSQL,POSTGRESQL, RDP, SIP, FTP, FTP-DATA, TFTP-DATA, SSL/TLS.	ano	Dodávané řešení je schopno vyhledávat v metadatech uvedených protokolů.
POŽ_1_14_04	Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	ano	Splňuje minimálně dle funkčního požadavku.
Požadavky na získávání a vizualizaci kontextových informací			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_15_01	Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace: • hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu; • IP geolokace; • IP reputace, vč. informace jestli je IP adresa na blacklistu nebo podezřelá; • historie použitých MAC adresa a výrobce zařízení; • operační systém a jeho historie na zařízení; • uživatelem zadané poznámky a informace k zařízení; • automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště,	ano	Zobrazení kontextu zařízení (hostname, OS, MAC, tagy, poznámky, reputace).

	aktivní dohledy, skenery zranitelností a technologické systémy.		
Požadavky na Zaznamenávání a ukládání plného provozu			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_16_01	Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech mezi všemi monitorovanými zařízeními, minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	ano	Volitelné full PCAP záznamy dle filtrů, na základě automatického nebo ručního spouštění.
Požadavky na nastavování a kontrolu bezpečnostních politik			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_17_01	Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně: • monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase; • detekovat změny v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru;	ano	Splňuje minimálně dle funkčního požadavku.
POŽ_1_17_02	Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: • uživatelem definované podsítě na základě rozsahů IP adres; • uživatelsky libovolně definovaných skupin zařízení; • automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	ano	Splňuje minimálně dle funkčního požadavku.

Požadavky na integraci			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_18_01	Zadavatel požaduje v rámci implementace Řešení i integraci se stávající firewallovou infrastrukturou od výrobce Fortinet v takové míře, aby bylo možné z nástroje automaticky blokovat detekovaný nechtěný síťový provoz.	ano	Automatická reakce a blokace provozu skrze FortiGate pomocí Fortinet Security Fabric.



Obrázek 1 – POŽ_1_07_02 – Blokové schéma

1.3.2 Licence síťové sondy

Požadavky na licence / subskripce			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_1_19_01	Zadavatel požaduje potřebné licenční pokrytí tak, aby byly splněny požadavky ve verifikační tabulce výše po dobu 2 let od předání.	ano	Splňuje minimálně dle funkčního požadavku.

1.4 Implementace monitoringu provozu koncových bodů

Požadavky zadavatele:

Upgrade monitorovacího systému Zabbix a zavedení nových zařízení do monitoringu.

Cílem této části projektu je provést modernizaci a **rozšíření stávajícího dohledového systému ICT** infrastruktury města a výrazné rozšíření jeho monitorovacích kapacit **o více než 50 koncových 5G bodů**, které se nachází mimo hlavní infrastrukturu, tedy **mimo interní síť Zadavatele**. Prioritou zadavatele je zabezpečení a kvalitní dohled nad koncovými body mimo dosah vnitřního monitoringu (externí zařízení).

Zadavatel v současné době provozuje plně opensourcový **monitorovací systém Zabbix** (https://www.zabbix.com/true_open_source) v režimu „on-premise“, tedy vlastními prostředky a na vlastní infrastruktuře. S ohledem na citlivý provoz je tento model nutné zachovat. Součástí tohoto projektu je aktualizace stávajícího prostředí (zejména pro zajištění kompatibility) a také výrazné rozšíření monitorovacího systému dle níže uvedených funkčních požadavků.

Realizace bude probíhat podle uvedeného časového plánu s důrazem na minimalizaci rizik a zajištění kontinuity provozu.

Implementaci monitoringu provozu koncových bodů (dashboardy, reporting) budou zajišťovat specialisté O2 IT Services s.r.o., což je 100% dceřiná společnost dodavatele.

Obecné požadavky			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_2_01_01	Update stávajícího provozního monitoringu sítě v rámci všech částí projektu 5G na základě analýzy (předimplemetační analýzy neboli cílového konceptu pro nasazení dohledového nástroje) zpracované Dodavatelem a odsouhlasené Zadavatelem na začátku realizace této části VZ.V rámci update Zhotovitel zajistí minimálně: - Analýzu stávající konfigurace monitorovacího systému Plánování a testování upgradu na testovacím prostředí (klon systému) z důvodu minimalizace výpadku produkčního systému Otestování funkčnosti systému a kompatibility stávajících nastavení a šablon. Provedení upgradu na produkčním prostředí s minimálním výpadkem Zadavatel předpokládá, že bude proveden update na nejnovější stabilní verzi, tedy verzi 7.2 a novější.	ano	V závislosti na stávající verzi a výsledku analýzy celkového stavu bude vybrán nejvhodnější způsob upgrade na požadovanou poslední verzi. V součinnosti se Zadavatelem bude proveden test a ověření funkčnosti, následně pak upgrade na produkci.
POŽ_2_01_02	Vytvoření dashboardů a map pro jednotlivá zařízení a služby provozované v rámci 5G projektu dle požadavku Zadavatele, které budou	ano	Na základě výsledku analýzy a v ní specifikovaných požadavků budou vytvořeny dashboardy a mapy.

	specifikovány v rámci zpracování analýzy (cílového konceptu).		
POŽ_2_01_03	Nastavení oprávnění pro Zadavatelem definované skupiny uživatelů pro jednotlivé dashboardy a mapy.	ano	Na základě výsledku analýzy a v ní specifikovaných požadavků budou nastavena oprávnění Zadavatelem definovaným skupinám k jednotlivým mapám a dashboardům.
POŽ_2_01_04	Autentizace uživatelů musí být realizována napojením na LDAP databázi Zadavatele.	ano	Autentizace uživatelů bude napojena na stávající LDAP Zadavatele, podle výsledku analýzy bude určeno, zda pro řízení oprávnění budou využity doménové skupiny.
POŽ_2_01_05	Nasazení a úprava nezbytných SNMP templates, pro vyčítání informací ze zařízení připojených v 5G síti, rozsah bude upřesněn v rámci analýzy.	ano	Nejvhodnější způsob implementace SNMP monitoringu zařízení bude zvolen na základě výstupu z provedené analýzy a v průběhu instalace a konfigurace dohlížených zařízení.
POŽ_2_01_06	Instalace, konfigurace a napojení zobrazovacího serveru s prostředím otevřeného nástroje typu Grafana pro možnost publikace pohledů na provozní stavy z jednotlivých dashboardů monitorovaných zařízení externím subjektům (server v DMZ na který se budou připojovat ostatní subjekty města zapojené do 5G projektů).	ano	V DMZ prostředí Zadavatele za jeho součinnosti bude nainstalován a zprovozněn Grafana server, přes Zabbix API napojený na Zabbix server. Dodavatel předpokládá, že VM na kterých bude provozován Zabbix a Grafana bude zřízen v požadované konfigurace na virtualizační platformě Zadavatele.
Požadavky na rozsah monitoringu a konfiguračních prací			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_2_02_01	Dodavatel vytvoří souhrnný dashboard pro monitoring všech vzdálených 5G bodů a jejich technologických ukazatelů. Upřesnění monitorovaných ukazatelů proběhne v analýze. Výstupem bude hlavní dashboard, obsahující minimálně: mapou města, ve které budou zakresleny jednotlivé vzdálené fixně umístěné 5G body (v rámci 5G projektů) na základě jejich GPS souřadnic. Tedy v mapě zobrazované v dashboardu bude vidět skutečné umístění 5G bodů. Z této centrální mapy se bude	ano	Bude vytvořen souhrnný dashboard a jednotlivé provázané dashboardy pro konkrétní 5G uzly v rámci 5G projektu. Podřízené dashboardy budou dostupné na prokliknutí ze souhrnného dashboardu. Jednotlivé stavy dohlížených prvků budou barevně rozlišeny podle zadání. Podrobnější způsob a rozsah řešení bude určen až na základě úvodní

	možné prokliknout na detailní mapu každého dílčího 5G bodu. U každého 5G bodu budou zobrazeny technologické ukazatele definované v rámci analýzy. • přehledem zjištěných problémů, kdy u každého jednotlivého problému musí být viditelná jeho závažnost ve stupnici minimálně: ○ Kritický; ○ Závažný ○ Střední; ○ Upozornění; ○ Informace ○ Neurčeno; • Zobrazením aktuálního času. V případě náhlého překročení technologických ukazatelů monitorovaných zařízení nad/pod obvyklou mez, budou ty zařízení, u kterých překročení vzniklo barevně odlišena a v přehledu problémů budou zaznamenány jednotlivá překročení i s aktuálními hodnotami a procentuálním rozdílem oproti průměrným hodnotám za normálního stavu daného technologického ukazatele. Z hlavních map a dashboardů bude možné přistoupit přímo do podřazených map a dashboardů jednotlivých 5G koncových bodů v propojeném logickém celku, ve kterých budou sledována pouze zařízení náležející konkrétnímu 5G projektů. • Grafické zobrazení odkazů do podřazených map musí barevně reflektovat závažnost stavů vyskytujících se na dané podřazené mapě (dle výše uvedené stupnice). Další požadavky na podobu dashboardu budou upřesněny v rámci analýzy.		analýzy ve spolupráci se Zadavatelem.
POŽ_2_02_02	Zadavatel předpokládá rozdělení dohledovaných zařízení minimálně do 7 logických skupin dle, a to dle koncových uživatelů logických celků, případně správců monitorovaných zařízen nastavením přístupových práv pro jednotlivé skupiny uživatelů.	ano	Na základě podkladů Zadavatele budou vytvořeny skupiny dohlížených prvků a příslušné skupiny uživatelů a správců s požadovaným oprávněním k jednotlivým skupinám.
POŽ_2_02_03	Zadavatel předpokládá, že v rámci kyberbezpečnostního a vzdáleného dohledu nad 5G sítí bude zapotřebí napojení na monitoring různých typů technologií (min. 5G modemy, koncové kyberbezpečnostní prvky, koncové funkční body nebo čidla, síťové toky a výstupy ze síťové sondy pro konkrétní 5G koncový bod atd.).	ano	Upřesnění požadavků vyplyne z úvodní analýzy ve spolupráci se Zadavatelem. Bude zvolen nejvhodnější způsob napojení.

	Bude požadováno nastavení a přiřazení šablon (templates) pro monitoring každé skupiny zařízení.		
POŽ_2_02_04	Dle typu monitorovaného zařízení definovat klíčové metriky pro každou skupinu zařízení, nastavit monitoring klíčových metrik, ukládání jejich historie, testování funkcionality a nastavení prahových hodnot pro notifikační upozornění (alarmy) a to zejména datových přenosů, přenosových parametrů, provozní teploty, zatížení CPU, případně dalších dle upřesnění v rámci analýzy.	ano	Upřesnění požadavků a způsob řešení bude určen až na základě úvodní analýzy ve spolupráci se Zadavatelem.
Požadavky na infrastrukturu a servisní zajištění			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_2_03_01	Na základě analýzy Zhotoviteli zajistí: • Instalaci a konfiguraci obslužného software pro monitoring v odpovídající konfiguraci a potřebném počtu • Přenesení stávající konfigurace systému a vytvoření nové konfigurace pro odpovídající monitoring dle zadávacích podmínek a dle specifikace v analýze • Další práce vyplývající z této zadávací dokumentace a výstupů analýzy Zadavatel disponuje vlastní virtualizovanou infrastrukturou, a zajistí: • Dostatečný výpočetní výkon serveru pro novější verzi dohledového systému • Zajištění zálohování • Dostupnost přístupu k nově monitorovaným zařízením • Licenční pokrytí virtualizace a operačního systému Windows / Linux.	ano	Rozsah a postup řešení bude určen až na základě úvodní analýzy ve spolupráci se Zadavatelem.
Časový harmonogram a očekávané výstupy			
ID požadavku	Funkční požadavek	Dodavatel splňuje (ANO/NE)	Popis způsobu plnění
POŽ_2_04_01	Zadavatel předpokládá následující harmonogram: • Analýza a příprava (s možností navýšení systémových prostředků) - 2 týdny • Testovací upgrade a validace funkčnosti stávajících nastavení a šablon. - 2 týdny • Produkční upgrade - 1 týden • Integrace nových zařízení - 3 týdny • Konfigurace dashboardů a map - 2 týdny • Testování a optimalizace - 2 týdny	ano	Skutečnou pracnost zjistíme až na základě úvodní analýzy a upřesnění požadavků Zadavatele, jak je zmíněno v předcházejících bodech.

POŽ_2_04_02	**Očekávané výstupy z Implementace monitoringu provozu koncových bodů – dashboardy, reporting:** • Aktualizovaná verze monitorovacího systému Zadavatele v produkčním prostředí • Monitorování nových zařízení z 5G projektů rozdělených do minimálně 7 logických skupin • Samostatné dashboardy a mapy pro každou skupinu. • Dokumentace k nastavení a konfiguraci. • Funkční a otestovaný monitoring (akceptační testování) • Dílčí akceptační protokol na předání díla dle cílového konceptu	ano	Vše podstatné již bylo uvedeno výše, ke všem dodaným částem bude předána odpovídající dokumentace a připraven akceptační protokol jako výsledek testů.

Tento odstavec bude sloužit jako podklad pro implementaci upgradu Zabbixu a zavedení nových zařízení do monitoringu. Realizace bude probíhat podle zde uvedeného časového plánu s důrazem na minimalizaci rizik a zajištění kontinuity provozu.

1.5 Pokročilé 5G routery

Požadavky zadavatele:

Na uvedených měnírnách je v současné době realizováno ovládání pouze po zastarávajícím rádiovém spojení, které se vyznačuje velkou mírou nespolehlivosti a frekventovanými výpadky. Zadavatel požaduje dodávku a implementaci 5G routerů umožňující připojení klíčových zájmových bodů a strategické infrastruktury.

U každé instalační lokality je nutné prověřit, zda bude fungovat anténa umístěná v rozvaděči nebo bude nutné kvůli kvalitě signálu instalovat externí anténu na rozvaděč. Router bude umístěn ve společném kamerovém rozvaděči, který bude instalován v rámci dodávky.

Router bude plnit roli zařízení typu inteligentní 5G gateway, s podporou přenosu dat pomocí encapsulace do šifrovaných datových toků v souladu s minimálními požadavky na kryptografii dle NUKIBu napříč 5G sítí operátora – k zajištění ochrany dat před odposlechem z infrastruktury poskytovatelů jednotlivých APN.

Encapsulace bude zajištěna sestavením site-to-site šifrovaných VPN tunelů pro jednotlivé služby a aplikace (tedy více tunelů mezi datovým centrem a vzdálenou lokalitou v rámci jednoho připojení 5G), ze vzdálené lokality na segmentační Firewall v datovém centru Metropolnetu.

Požadavek zadavatele	Nabízené řešení splňuje (ano/ne)	Poznámka
Dodání celkem 16 pokročilých 5G routerů vč. 16 5G SIM	ano	Budou dodány 5G routery ICR 4461, produktový list k routerům předložil dodavatel ve své nabídce.

Podpora technologie 5G NR v souladu se standardem 3GPP	ano	
Router garantující přenosové parametry odpovídající požadavkům poptávaného aplikačního řešení	ano	
Datový limit odpovídající přenosovým potřebám aplikačního řešení (optimálně neomezený)	ano	
Potřebné doplňkové příslušenství (antény, kabely, úchyty, zdroje) pro zajištění optimálního výkonu	ano	
Podpora min. 2 SIM slot (min. 1x 5G SIM musí být součástí řešení)	ano	
Přijímač GNSS signálu s podporou GPS a Galileo	ano	
Minimálně 3x Ethernet 10/100/1000 s PoE	ano	
Doplnění o externí antény pro maximalizaci kvality signálu	ano	
Možnost nahrávání vlastních aplikací (vybavení paměťovým prostorem), podpora Python a Docker	ano	
Vlastní Wi-Fi (MIMO antény)	ano	
Ochrana zařízení min. IP30	ano	
Bezpečnostní prvky: VPN Tunneling IPsec Site-to-Site, šifrování, firewall, HTTPS, SSH	ano	
Rozsah provozní teploty min. -40°C až + 70°C	ano	
Možnost automatických vzdálených aktualizací firmware	ano	
Dodávka musí zahrnovat veškeré potřebné licence a SW pro provoz a správu zařízení	ano	
Podpora IEEE 802.1Q (VLAN), SNMP, SNMP-trap	ano	
L3 routing s možností doplňování statických rout	ano	
Možnost nastavení v L3 routing provozu s NAT a bez NAT (minimálně s touto možností na WAN/5G interface)	ano	

1.6 Konektivita 5G dle specifikací 3GPP

Dodavatel zajistí zprovoznění a konfiguraci 5G sítě, integrační služby, konektivitu pro zařízení a provoz sítě.

Požadavky zadavatele:

Zadavatel požaduje zajištění služeb vytvoření, dodání a vstupní konfigurace zabezpečené 5G konektivity pro potřeby provozu technologického řešení (resp. koncových prvků demonstrativní aplikace).

Předpokládané plnění zahrnuje nejen samotné zajištění konektivity, ale rovněž veškerou nutnou součinnost pro propojení do sítě zadavatele a připojení koncových zařízení do sítě.

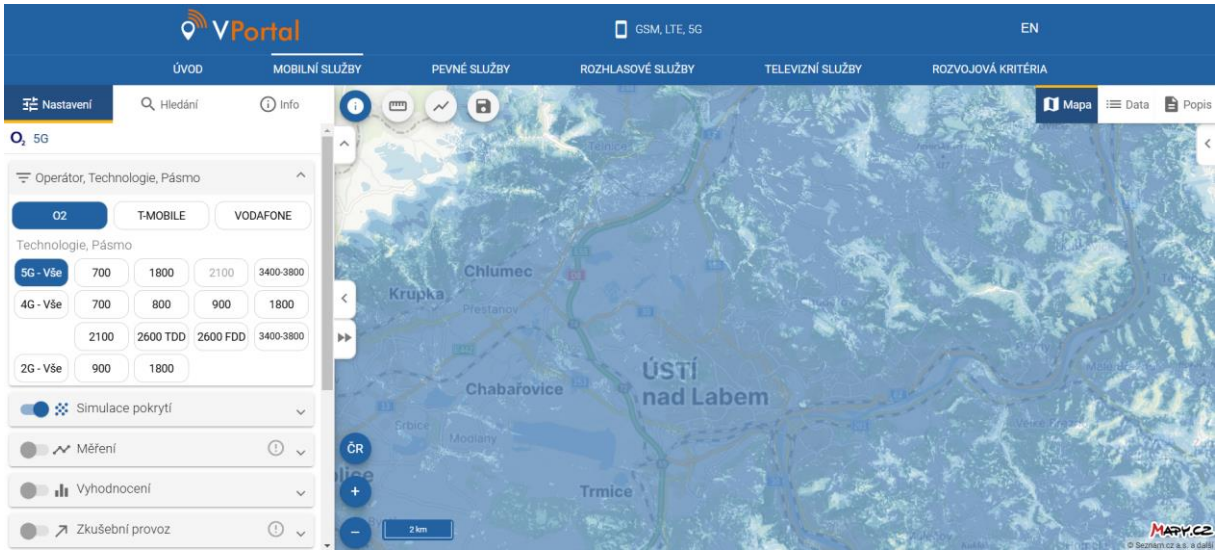
Technologické vybavení bude pomocí zřízené neveřejné sítě připojeno na speciálně definovaný APN (Access Point Name), přičemž zřízení a provoz APN je předmětem této zakázky. Dodavatel zajistí pomocí zabezpečené neveřejné sítě propojení na síť a infrastrukturu zadavatele. Zadavatel požaduje možnost použít vlastní IP adresy koncových zařízení – konfigurace neveřejné sítě je součástí plnění.

Požadavek zadavatele	Nabízené řešení splňuje (ano/ne)	Poznámka
Poskytování datových služeb – zřízení, konfigurace, provoz a zpřístupnění privátní APN do sítě 5G	ano	
Požadavek na dodržení specifikací 3GPP	ano	5G O2: n28 (5GNR700), n3 (5GNR1800), n78 (5GNR 3700)
Poskytování služeb 5G konektivity pro koncová zařízení (16 routerů) po dobu trvání projektu (předpoklad: max. 12 měsíců, fakturace dle skutečného čerpání konektivity na měsíční bázi, modelové nacenění pro potřeby nabídkové ceny – 12 měsíců)	ano	
Zřízení, konfigurace, nastavení a provoz neveřejné sítě pro připojení bodů koncových sítě na APN	ano	
Konfigurace pokročilých 5G routerů, nastavení propojení s technologiemi aplikačního řešení	ano	
Propojení a konfigurace koncových bodů aplikačního řešení na operační středisko MPÚL	ano	
Služby provozu, podpory provozu a servisu dodaného řešení	ano	
Zabezpečení: IPsec VPN musí být omezena pouze na IP adresu koncentrátoru poskytovatele	ano	
Ověřování pro navázání zabezpečeného tunelu musí být na základě certifikátu	ano	
Ochrana proti připojení cizího zařízení	ano	Dedikované APN + Radius server O2 (autentizace: jméno a heslo)
Součinnost se zástupci zadavatele při integraci inovativních prvků kybernetického zabezpečení	ano	
Datové tarify odpovídající potřebám provozu aplikačního řešení, optimálně neomezený FUP	ano	IP Connect Mobile Access 5G – neomezený datový tarif (bez FUP)
Nepředpokládá se 24/7 datový přenos	ano	Dodavatel bere na vědomí

Aktuální podrobná mapa pokrytí signálem je na webových stránkách poskytovatele a dále také na webu ČTÚ (viz odkazy níže).

O2 | Mapa pokrytí

ČTÚ Vizualizační Portál – Mobilní služby (ctu.cz)



Tabulka 1 - Pokrytí 4G a 5G mobilní sítě poskytovatele O2 (data dle ČTÚ ze dne 15.4.2025)

Mobilní síť	Pokrytí území – Ústí nad Labem	Pokrytí obyvatel – Ústí nad Labem
4G	99,89 %	99,94 %
5G	99,76 %	99,98 %

1.7 Další požadavky předmětu plnění veřejné zakázky

Požadavek zadavatele	Nabízené řešení splňuje (ano/ne)	Poznámka
Účastník je v rámci nabídky povinen předložit návrh přístupu k plnění předmětu veřejné zakázky a prokázat naplnění minimálních technických požadavků například formou technické dokumentace, produktových listů apod.).	ano	Návrh přístupu k plnění předmětu zakázky a prokázání naplnění minimálních technických požadavků jsou uvedeny v odst. 4.1 až 4.7 této nabídky.
Součástí předmětu plnění jsou také služby projektového vedení předmětu plnění veřejné zakázky na straně dodavatele:		
• Dodavatel zajistí projektové vedení plnění předmětu veřejné zakázky po celou dobu realizace dodávky prostřednictvím projektového manažera, který bude v průběhu plnění předmětu veřejné zakázky aktivně a konstruktivně komunikovat s jmenovaným zástupcem zadavatele.	ano	Dodavatel alokuje certifikovaného projektového manažera, dle mezinárodních standardů.

• Součástí služeb projektového vedení je také proaktivní vyžádání si součinnosti a koordinace prací, služeb a/nebo dodávek třetích stran (zejm. stávajících a/nebo paralelně plnících nových dodavatelů zadavatele) zapojených do plnění předmětu této veřejné zakázky nebo poskytujících plnění navazující a/nebo ovlivňující plnění této veřejné zakázky za účelem dosažení úspěšné realizace předmětu plnění této veřejné zakázky jako celku a jeho úspěšné realizace v daném časovém rámci vč. jednotlivého oprávněného konkrétního úkolu s určeným termínem z kontrolního dne v rámci koordinace prací, služeb a/nebo dodávek	ano	Dodavatel počítá s proaktivní spoluprací, v oblasti iniciace nezbytných součinností a koordinace napříč realizačním týmem.
• Pro účely kontroly průběhu provádění předmětu plnění této veřejné zakázky bude dodavatel organizovat kontrolní dny – kontrolní dny se budou konat za účasti zástupců smluvních stran min. 1 x 14 dní. Dodavatel zajistí řízení všech kontrolních dnů a dílčích jednání s administrátory, uživateli a vedením projektu na straně zadavatele. Z kontrolního dne provede dodavatel písemný zápis. Dodavatel je povinen se řádně svolaného kontrolního dnu zúčastnit. Změna termínů a stanovení periodicity termínů kontrolních dnů je výhradně na straně zadavatele.	ano	
• Dodavatel dále zajistí zpracování harmonogramu prací v podobě navazujících činností, např. formou Ganttova diagramu nebo MS Project, či obdobného nástroje postihující návaznosti ke všem částem plnění	ano	Podrobný harmonogram, na období po nabytí účinnosti Smlouvy o Dílo, zpracován – viz bod 7
• Dodavatel zajistí řízení vzniku veškeré administrátorské, provozní, bezpečnostní, uživatelské dokumentace, školících materiálů, organizace školení samotného a další projektové dokumentace	ano	Školení bude zajištěno dle požadavku zadavatele stanoveného v Oddíle II. Smlouvy o dílo, bod 7. *
• Dodavatel zajistí veškeré řídící činnosti projektu s vlastníky projektu na straně zadavatele nebo jím určených třetích stran na straně dodavatele	ano	
Zadavatel požaduje od dodavatele součinnost a ad hoc spolupráci s dodavateli dalších, paralelně realizovaných VZ v rámci řešeného 5G projektového záměru, a to po celou dobu plnění.	ano	

V případě dodávky technologií (materiálů a komponent) nezbytných pro plnění veřejné zakázky musí být vždy předmětem dodávky zařízení nové, nepoužité, nerepasované, nezastavené, nezapůjčené, nezatížené leasingem ani jinými právními vadami a nesmí porušovat žádná práva třetích osob k patentu nebo k jiné formě vlastnictví jako takového.	ano	
Součástí dodávky musí být také příslušné atesty použitých materiálů a doklady o požadovaných vlastnostech výrobků (včetně případných prohlášení o shodě dle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, v platném znění) u výrobků a materiálů, u nichž je to obvyklé, plán revizí elektronických zařízení, provozní řád dodaných technologií a podklady pro stanovení intervalů údržby a čištění apod.	ano	
Na veškeré dodané hardwarové a softwarové vybavení (včetně počítačů, analytického softwaru a dalšího příslušenství) se požaduje minimální záruka v délce 24 měsíců v souladu se zákonem č. 89/2012 Sb., občanský zákoník. Tato záruka zahrnuje právo na opravu nebo výměnu zařízení v případě zjištěných vad, které existovaly při převzetí nebo se projevily v záruční době. Vady, které se objeví během prvních 12 měsíců, se považují za vady existující již při převzetí, pokud prodávající neprokáže opak.	ano	

* Školení personálu zadavatele: V souladu s Oddílem II. Smlouvy o dílo, bod 7. zajistí dodavatel školení personálu v rozsahu nezbytném pro zvládnutí každodenní správy a používání, a to v rozsahu 12 hodin, pro maximálně 8 osob. Školení proběhne v prostorách sídla zadavatele, v termínu stanoveném zadavatelem. Termín školení bude stanoven v souladu s Harmonogramem v kapitole 7 této nabídky.

2. Harmonogram

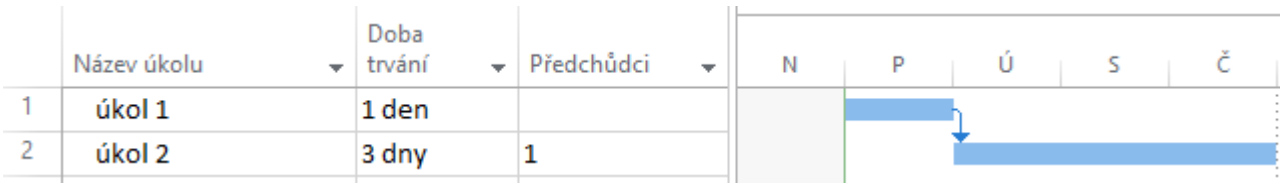
Harmonogram respektuje klíčové milníky, ze zadávací dokumentace VZ. Nebude-li dohodnuto jinak, veškerá činnost na projektu je uvažována, výhradně v rámci obvyklé pracovní doby – tj. 8-17hod.; rozmezí běžného pracovního týdne: pondělí – pátek

Doby trvání jednotlivých úkolů v uvedeném časovém harmonogramu, jsou proto rovnou uvedeny v pracovních dnech.

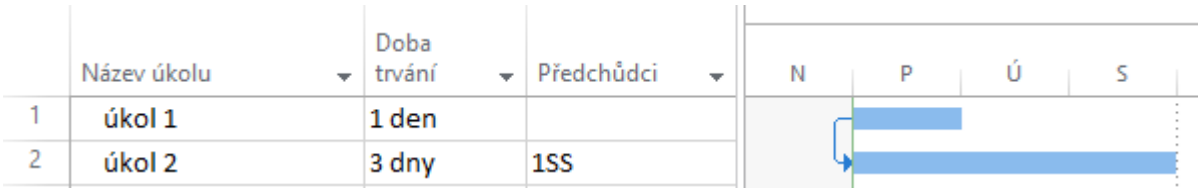
V harmonogramu jsou použity jen vzájemné vazby propojení mezi jednotlivými úkoly, a to typu „finish => start“ a „start => start“.

Vysvětlení vazeb mezi úkoly:

- „finish => start“: následný úkol může být zahájen pouze poté, co předchozí úkol byl dokončen (průběh formou kaskády) – viz obr.



- „start => start“: následný úkol je zahájen zároveň s předchozím úkolem (paralelní průběh) – viz obr.



Harmonogram – chronologický seznam úkolů, vč. doby trvání a vzájemných vazeb mezi nimi

ID	Číslo osnovy	Název úkolu	Doba trvání	Předchůdci	Následníci
1	**1**	**Ústí nad Labem_KYBEZ/5G**	**110 dny**		
2	1.1	Nabytí účinnnosti smlouvy	0 dny		3;11
3	1.2	Úvodní projektová schůzka	5 dny	2	4
4	1.3	Provedení předimplementační analýzy a její schválení zadavatelem	15 dny	3	14;12;13;7;8;9;10;15
5	**1.4**	**Dodávka technologií**	**45 dny**		**16**
6	**1.4.1**	instalace do rozvaděčů	**45 dny**		**15**
7	1.4.1.1	kamery	45 dny	4	
8	1.4.1.2	5G routery	45 dny	4	10SS;12SS
9	1.4.2	Síťové sondy	45 dny	4	13SS
10	1.5	Zpřístupnění a konfigurace 5G sítě	45 dny	4;8SS	
11	**1.6**	**Konfigurační práce**	**54 dny**	**2**	**16;15**
12	1.6.1	APN	10 dny	4;8SS	
13	1.6.2	Síťové sondy	50 dny	4;9SS	
14	1.6.3	Zabbix	54 dny	4	
15	1.7	Dokončení školení, předání dokumentace	5 dny	4;6;11	16
16	1.8	Testovací provoz	20 dny	5;11;15	17
17	1.9	Prokázání funkčnosti aplikačního řešení v souladu s cíli Projektu 5G	10 dny	16	18
18	1.10	Formální předání, fakturace a ukončení plnění – závazný termín	0 dny	17	19
19	1.11	Čerpání služeb (technická podpora, licence, konektivita)	1 den	18	

Harmonogram – Ganttův diagram