Smlouva o poskytování služeb operátora MSpWAN
č. MPS-20/2025-MSP-CES

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (**„Smlouva“**)

SMLUVNÍ STRANY

(1) **Česká republika – Ministerstvo spravedlnosti**

se sídlem na adrese	Vyšehradská 16, Praha 2, PSČ: 128 00
IČO:	00025429
bankovní spojení:	Česká národní banka
číslo účtu:	5120001/0710
zastoupená:	Ing. Bc. Radomírem Daňhelem MBA, LL.M., náměstkem člena vlády poměřeným v oblasti ekonomické a správní

(„**Objednatel**“)

(2) **ALEF NULA, a.s.**

se sídlem na adrese	Pernerova 691/42, Karlín, 186 00 Praha 8
společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze vložka B, oddíl 2727	
IČO:	61858579
DIČ:	CZ61858579
bankovní spojení:	Komerční banka, a.s.
číslo účtu:	51-3717150237/0100
zastoupená:	Ing. Milanem Zinkem, předsedou představenstva

(„**Poskytovatel**“)

(Objednatel a Poskytovatel společně jen „**Strany**“ a každý z nich samostatně „**Strana**“)

PREAMBULE

A. Objednatel oznámil v otevřeném zadávacím řízení ve smyslu § 56 a násl. zákona č. 134/2016Sb. o zadávání veřejných zakázek, ve znění pozdějších předpisů („**ZZVZ**“), svůj úmysl zadat v tomto řízení nadlimitní veřejnou zakázku na služby s názvem „***Poskytování služeb operátora MSpWAN***“ („**Veřejná zakázka**“), jejímž předmětem je zajistit pro Objednatele dlouhodobé užívání služeb WAN (Wide Area Network) infrastruktury z části vybudované a provozované Poskytovatelem („**Infrastruktura MSpWAN**“). Na základě zadávacího řízení na Veřejnou zakázku Poskytovatel předložil nabídku v souladu se zadávacími podmínkami veřejné zakázky a tato byla pro plnění veřejné zakázky vybrána jako nejvhodnější. V návaznosti na tuto skutečnost Strany uzavírají tuto Smlouvu, jejíž návrh byl součástí zadávacích podmínek Veřejné

zakázky.

B. Poskytovatel je odborníkem ve smyslu zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů („**Občanský zákoník**“) v oboru informatika a výpočetní technika se zvláštní specializací na návrh, výstavbu a provoz počítačových sítí velkého rozsahu a prohlašuje, že má veškeré dostupné požadované znalosti a nejnovější relevantní zkušenosti v oblasti budování a provozování moderní generace dálkové sítě WAN pro realizaci Objednatelem požadovaného plnění. Poskytovatel je proto připraven plnit své povinnosti vyplývající ze Smlouvy a realizovat předmět Veřejné zakázky v souladu s principy „*best practice*“ dle svého nejlepšího vědomí, ve prospěch Objednatele a s ohledem na úsporu nákladů Objednatele.

C. Poskytovatel si je vědom

- významu a důležitosti plné funkčnosti Infrastruktury MSpWAN pro Objednatele a jeho organizační složky,
- skutečnosti, že dostupnost Infrastruktury MSpWAN je významným faktorem ve výkonu veřejné moci v České republice a
- skutečnosti, že vady plnění dle této Smlouvy mohou mít za následek mimořádně závažné dopady pro veřejnou správu České republiky, soudnictví i bezpečnost státu.

S vědomím těchto skutečností odpovědně přijímá závazky ze Smlouvy a je připraven řádně realizovat předmět Veřejné zakázky.

1. Účel a předmět Smlouvy

1.1 Účelem Smlouvy je úprava a vymezení podmínek pro realizaci a plnění Veřejné zakázky dle zadávací dokumentace pro Veřejnou zakázku („**Zadávací dokumentace**“) a s tím související stanovení podmínek, za kterých bude Poskytovatel poskytovat Objednateli plnění specifikované blíže v odst. 1.2 a v odst. 1.3 tohoto Článku Smlouvy za účelem dlouhodobého zajištění užívání služeb Infrastruktury MSpWAN k zajištění kapacitní, bezpečné, vysoce spolehlivé a technologicky relevantní konektivity mezi Objednatelem, organizačními složkami nebo třetími stranami a umožnění vysoké míry interoperability mezi nimi (**„Služby Infrastruktury MSpWAN“**).

Účelem Smlouvy je rovněž zakotvit technické a organizační podmínky provozu Infrastruktury MSpWAN, způsob jejího řízení, dohledu nad ní, jejího rozšiřování či změn a další související otázky.

Účelem Smlouvy je tak splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle Zadávací dokumentace. Ustanovení Smlouvy, jejích Příloh a Zadávací dokumentace budou vykládána tak, aby jednotlivá ustanovení obstála, pokud možno vedle sebe bez nutnosti vyloučení jednoho ustanovení jiným.

1.2 Předmětem této Smlouvy je závazek Poskytovatele poskytovat Objednateli plnění sestávající z implementace, udržování a provozování Infrastruktury MSpWAN specifikované v odst. 1.3 tohoto Článku a v Přílohách č. 1 [*Technická specifikace*] a č. 2 [*Úroveň servisních služeb (SLA)*], tak aby bylo zajištěno plnění Služeb Infrastruktury MSpWAN za podmínek stanovených touto Smlouvou („**Služby**“).

Předmětem Smlouvy je rovněž závazek Objednatele hradit Poskytovateli za řádně poskytnuté plnění cenu dle Článku 4 Smlouvy.

1.3 Služby zahrnují zejména:

(i) **Instalaci a konfiguraci komunikačních center**

Instalace a konfigurace komunikačních center spočívá ve vybudování komplexní Infrastruktury MSpWAN v souladu s Přílohou č. 1 [*Technická specifikace*].

Instalace a konfigurace komunikačních center bude realizovaná v souladu se schváleným Implementačním projektem.

V rámci Instalace a konfigurace komunikačních center zajistí Poskytovatel příslušná užívací a související oprávnění za účelem možnosti plného užívání Infrastruktury MSpWAN a Služeb Infrastruktury MSpWAN Objednatelem a jeho organizačními složkami.

Poskytovatel je povinen zajistit příslušná oprávnění dle předchozí věty pro celou dobu trvání Smlouvy.

(ii) **Služby provozu**

V rámci Služeb provozu Poskytovatel zajistí bezproblémové fungování Infrastruktury MSpWAN a poskytování Služeb Infrastruktury MSpWAN.

Poskytovatel bude poskytovat Služby provozu v souladu s Přílohou č. 1 [*Technická specifikace*] a Přílohou č. 2 [*Úroveň servisních služeb (SLA)*] od prvního dne měsíce následujícího po podepsání Akceptačního protokolu dle Článku 5 Smlouvy („**Den zahájení poskytování služeb provozu**“).

Služby provozu budou poskytované po dobu 10 let ode Dne zahájení poskytování služeb provozu.

(iii) **Udržování a zpřístupnění dokumentace**

Poskytovatel je povinen průběžně udržovat dokumentaci tak, aby byla aktuální a odpovídala skutečnému provedení Infrastruktury MSpWAN a poskytovaným Službám Infrastruktury MSpWAN (dále jen „**Dokumentace**“).

Poskytovatel je povinen po celou dobu trvání Smlouvy udržovat kompletní aktuální dokumentaci celé Infrastruktury MSpWAN tak, aby bylo dostatečně přesně patrno zejména:

(a) jakými prvky a jakého typu a sériových čísel je Infrastruktura MSpWAN tvořena;

(b) v jakých Implementačních lokalitách či na jiných místech jsou tyto prvky fyzicky umístěny;

(c) jaká je topologie Infrastruktury MSpWAN;

(d) jaký software je pro provoz Infrastruktury MSpWAN užíván, kde a jakým způsobem;

(e) jaké přístupové údaje jsou používány ke správě Infrastruktury MSpWAN na všech jejích úrovních;

(f) jaká napojení na služby poddodavatelů jsou pro provoz Infrastruktury MSpWAN potřebná, včetně poddodavatelských smluv.

Po celou dobu účinnosti Smlouvy:

- musí být aktuální verze Dokumentace nepřetržitě dostupná Objednateli zabezpečeným dálkovým přístupem;
- přehled přístupových údajů dle písm. (e) shora s právem čtení (read-only) musí být nepřetržitě přístupný pro Objednatele na základě jeho žádosti, a to především za účelem kontroly bezpečnosti a nastavení zařízení a Infrastruktury MSpWAN;
- je Poskytovatel povinen zajistit pravidelné zálohy aktuální verze Dokumentace dle požadavků Objednatele.

(iv) **Zaškolení**

Účelem zaškolení je seznámit vybrané zaměstnance Objednatele/organizačních složek Objednatele s Infrastrukturou MSpWAN a Službami Infrastruktury MSpWAN.

(v) **Oprávnění k výstupům dodaným Poskytovatelem**

Poskytovatel uděluje Objednateli v souladu s Článkem 11 Smlouvy neomezená oprávnění ke všem výstupům, které vytvořil v rámci plnění předmětu Smlouvy, vlastní k nim autorská práva a předal je Objednateli („**Výstupy Poskytovatele**“).

Objednatel je oprávněn s Výstupy Poskytovatele neomezeně nakládat, modifikovat je a využívat je dle svého uvážení, a to z části nebo plně.

2. Místo a doba plnění Smlouvy

2.1 Místem plnění Smlouvy jsou lokality Objednatele a organizačních složek Objednatele, jejichž seznam ke dni podpisu Smlouvy tvoří Přílohu č. 4 [*Seznam a kategorizace Implementačních lokalit*] („**Implementační lokality**“).

2.2 Strany sjednávají, že Implementační lokality, resp. Seznam a kategorizace Implementačních lokalit bude v době trvání Smlouvy Objednatelem upravován dle aktuálních potřeb.

Poskytovatel je povinen poskytovat plnění pro Implementační lokality dle upraveného/doplněného Seznamu a kategorizace Implementačních lokalit vždy od 1. dne druhého kalendářního měsíce následujícího po předání upraveného/doplněného Seznamu a kategorizace Implementačních lokalit Poskytovateli.

O předání upraveného/doplněného Seznamu a kategorizaci Implementačních lokalit podepíší Strany předávací protokol.

2.3 Plnění Poskytovatele je rozděleno do těchto dvou fází:

1) Fáze Instalace a konfigurace komunikačních center,

2) Fáze Služeb provozu.

2.4 Fáze **Instalace a konfigurace komunikačních center**, začíná běžet ode dne následujícího po nabytí účinnosti Smlouvy a končí podpisem finálního akceptačního protokolu pro Fázi Instalace a konfigurace komunikačních center („**Finální akceptační protokol Instalace a konfigurace komunikačních center**“) s výrokem Objednatele „akceptováno“, přičemž trvání této fáze nesmí být delší než 18 měsíců od nabytí účinnosti Smlouvy.

Poskytovatel bude v této fázi průběžně budovat Infrastrukturu MSpWAN a zajišťovat poskytování Služeb Infrastruktury MSpWAN dle Přílohy č. 1 [*Technická specifikace*].

Komunikační centrum bude Poskytovatelem zřízeno na základě Objednatelem písemně schválené žádosti, jejíž vzor je v Příloze č. 3 [*Žádost o zřízení komunikačního centra*].

Poskytovatel a Objednatel/organizační složka Objednatele podepíšou po Instalaci a konfiguraci každého komunikačního centra dílčí akceptační protokol („**Dílčí akceptační protokol Instalace a konfigurace komunikačního centra**“), přičemž Instalace a konfigurace komunikačního centra se má za provedenou podpisem takového akceptačního protokolu s výrokem Objednatele „akceptováno“.

Poskytovatel je povinen v této fázi provést instalaci a konfiguraci všech komunikačních center u Objednatele a organizačních složek Objednatele tak, aby nejpozději ke dni podpisu Finálního akceptačního protokolu Instalace a konfigurace komunikačních

center vznikla Infrastruktura MSpWAN a byly zprovozněné všechny Služby Infrastruktury MSpWAN.

Poskytovatel se zavazuje při realizaci Instalace a konfiguraci komunikačního centra dodržet termíny písemně dohodnuté s Objednatelem nebo organizační složkou Objednatele. Pokud Objednatel nebo organizační složka Objednatele neposkytne definovanou součinnost v požadovaných lhůtách, sepíšou Strany o tomto Zápis o dalším postupu, v kterém dohodnou další postup. Zápis o úpravě termínů, požadavků na součinnost atd. musí být podepsán oběma Stranami.

2.5 Fáze **Služeb provozu**, začíná běžet od 1. dne následujícího měsíce po podpisu Dílčího akceptačního protokolu Instalace a konfigurace komunikačního centra s výrokem Objednatele „akceptováno“ dle Článku 2 odst. 2.34 Smlouvy („**Den spuštění pro konkrétní komunikační centrum**“) a skončí uplynutím 10 let (120 měsíců) ode dne podpisu Finálního akceptačního protokolu Instalace a konfigurace komunikačních center dle Článku 2 odst. 2.34 Smlouvy.

Poskytovatel bude v této Fázi Služeb provozu poskytovat služby specifikované v Příloze č. 1 [*Technická specifikace*] a Příloze č. 2 [*Úroveň servisních služeb (SLA)*].

3. Požadavky na změny nastavení Infrastruktury MSp WAN nebo Služeb

3.1 Požadavek na změnu nastavení Infrastruktury MSpWAN nebo Služeb Infrastruktury MSpWAN („**Změna služby**“) bude zadáván tak, že Objednatel nebo oprávněný zástupce organizační složky Objednatele nejprve zašle Poskytovateli písemný požadavek na změnu („**Požadavek**“), ve kterém bude uvedena požadovaná změna, specifikace Implementační lokality dle Přílohy č. 4 [*Seznam a kategorizace Implementačních lokalit*] a označení kontaktní osoby Objednatele nebo oprávněné osoby za organizační složku a její kontaktní údaje.

Strany se dohodly, že Požadavek bude Poskytovateli zasílán Objednatelem prostřednictvím ServiceDesk systému Poskytovatele dle Přílohy č. 2 [*Úroveň servisních služeb (SLA)*].

3.2 Poskytovatel prostřednictvím ServiceDesk systému potvrdí e-mailem na adresu kontaktní osoby Objednatele/organizační složky uvedené v příslušném Požadavku ve lhůtě uvedené v Příloze č. 2 [*Úroveň servisních služeb (SLA)*] přijetí Požadavku („**Zadání Požadavku**“).

3.3 Vyžaduje-li Změna služby Poskytovatelem nutnost dalších informací či součinnost ze strany Objednatele či organizační složky Objednatele, je Poskytovatel povinen si je od Objednatele/organizační složky vyžádat. Neučiní-li tak, má se za to, že informace uvedené v Požadavku a stávající připravenost jsou pro Poskytovatele dostačující a

nemůže se z tohoto důvodu zprostit odpovědnosti za nesplnění či vadné poskytnutí Služby („**Akceptace Požadavku**“).

3.4 Po Akceptaci Požadavku je Poskytovatel povinen zahájit řešení Požadavku a vyřešit Požadavek v souladu a ve lhůtách dle Přílohy č. 2 [*Úroveň servisních služeb (SLA)*].

3.5 Objednatel není oprávněn požadovat po Poskytovateli poskytnutí služeb, které svou povahou a charakterem zásadně vybočují z charakteru a podstaty této Smlouvy, nebo jejichž poskytnutí představuje zvýšené náklady zásadně nesrovnatelné s náklady na poskytování Služeb specifikovaných v této Smlouvě.

4. Cena Služeb a platební podmínky

4.1 Za řádné poskytování Služeb dle této Smlouvy se Objednatel zavazuje hradit Poskytovateli cenu, a to za podmínek stanovených níže v tomto Článku 4.

4.2 Ceny za poskytování Služeb pro konkrétní kategorii komunikačního centra za jeden (1) kalendářní měsíc jsou sjednány následovně:

Cena Služeb pro jedno	**Cena bez DPH**	**Sazba DPH v %**	**Částka DPH**	**Cena včetně DPH**
Komunikační centrum Hlavní dle Přílohy č. 1A	1 213 200 Kč	21%	254 772 Kč	1 467 972 Kč
Komunikační centrum Velké dle Přílohy č. 1B	117 600 Kč	21%	24 696 Kč	142 296 Kč
Komunikační centrum Střední dle Přílohy č. 1C	30 700 Kč	21%	6 447 Kč	37 147 Kč
Komunikační centrum Malé dle Přílohy č. 1D	5 300 Kč	21%	1 113 Kč	6 413 Kč

(společně jen „**Cena Služeb**“).

4.3 Cena za poskytování Služeb za jeden (1) kalendářní měsíc ode Dne spuštění pro konkrétní komunikační centrum uvedená v odst. 4.2 tohoto Článku je stanovena částkou zahrnující veškeré plnění obsažené ve Službách.

4.4 Poskytovatel je oprávněn fakturovat po skončení kalendářního měsíce v souladu s odst. 4.7 tohoto Článku částku odpovídající součinu skutečného počtu aktuálně provozovaných komunikačních center ve Fázi Služeb provozu (v souladu s Článkem 2.5 Smlouvy) a cen za poskytování Služeb pro příslušná komunikační centra uvedených v tabulce v odst. 4.2 tohoto Článku.

4.5 Cena Služeb bude Objednatelem hrazena pouze za kalendářní měsíce, v nichž byly poskytovány Služby provozu. Pokud Služby provozu nebyly poskytovány po celý kalendářní měsíc, bude platba příslušné Ceny Služeb za daný kalendářní měsíc snížena o alikvotní část.

4.6 Poskytovateli vzniká právo na zaplacení Ceny Služeb na základě řádně vystavené faktury.

4.7 Poskytovatel je oprávněn vystavit první fakturu po skončení kalendářního roku 2025, a to za Služby poskytnuté v rámci Fáze Služeb provozu v roce 2025, které byly schváleny, resp. došlo k akceptaci příslušných měsíčních výkazů (reportů) Služeb za dané kalendářní měsíce Objednatelem dle Článku 5 odst. 5.6 Smlouvy, přičemž náležitosti měsíčního výkazu jsou uvedeny v Příloze č. 6 [*Vzor Měsíčního výkazu*] („**Měsíční výkaz**“). Přílohou originálu Faktury musí být kopie příslušných Měsíčních výkazů písemně schválených Objednatelem.

4.8 Faktury za Služby provozu poskytnuté od 1. 1. 2026 je Poskytovatel oprávněn vystavit vždy po skončení daného kalendářního měsíce, ve kterém byly fakturované Služby poskytovány, a po akceptaci příslušného Měsíčního výkazu za daný kalendářní měsíc Objednatelem Přílohou originálu Faktury musí být kopie schváleného příslušného Měsíčního výkazu.

4.9 Ceny Služeb dle tohoto Článku 4 jsou, s výjimkami sjednanými v odstavci 4.10, nepřekročitelné a nejvýše přípustné a zahrnují veškeré náklady Poskytovatele spojené s plněním Služeb, včetně odměny za poskytnutí souvisejících oprávnění a licencí poskytovaných v souvislosti s plněním dle této Smlouvy, veškerého materiálu, práce, balení, poplatků, dopravy a doručení do míst dodání atd.

4.10 Změna Cen Služeb je přípustná v případě změny zákonem stanovené sazby DPH, na základě písemného dodatku, podepsaného k tomu oprávněnými zástupci obou Stran. K Cenám Služeb bez DPH se připočte daň z přidané hodnoty ve výši stanovené právními předpisy platnými ke dni uskutečnění zdanitelného plnění.

4.11 V souladu s Článkem 2 odst. 2.12 Smlouvy Strany sjednávají, že změna kategorizace Lokalit a/nebo navýšení počtu Lokalit, na kterých jsou/budou na základě Smlouvy poskytovány Služby, nemá vliv na výši Cen za poskytování Služeb pro konkrétní kategorii komunikačního centra uvedených v odst. 4.2 tohoto Článku.

4.12 Cena Služeb bude hrazena vždy na základě daňového dokladu – faktury („**Faktura**"), která musí obsahovat zejména:

(i) údaje v souladu s § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů;

(ii) údaje v souladu s § 435 Občanského zákoníku;

(iii) označení a číslo této Smlouvy;

(iv) povinnou přílohu, kterou je kopie Měsíčního výkazu schváleného Objednatelem (s dokladem o jeho schválení).

4.13 V případě vadného poskytnutí Služeb, je Poskytovatel povinen ve Faktuře uvést výši smluvní pokuty za Degradaci Služeb dle Článku 16 odst. 16.3 a/nebo za Nedodržení SLA dle Článku 16 odst. 16.4 a o výši této smluvní pokuty ponížit fakturovanou částku. Výše smluvní pokuty za Degradaci Služeb dle Článku 16 odst. 16.3 a/nebo za Nedodržení SLA dle Článku 16. odst. 16.4 bude uvedena v příslušném Měsíčním výkazu schváleném Objednatelem.

4.14 Lhůta splatnosti Faktur je třicet (30) dnů ode dne doručení příslušné Faktury Poskytovatele Objednateli. Faktury lze zasílat v písemné podobě poštou na adresu Objednatele, do datové schránky Objednatele nebo elektronicky (ve formátu PDF) se zaručeným elektronickým podpisem na e-mailovou adresu Objednatele [redacted]. Připadne-li termín splatnosti na den, který není pracovním dnem, posouvá se termín splatnosti na nejbližší následující pracovní den.

4.15 Objednatel má po obdržení Faktury třicet (30) dnů na posouzení toho, zda je bezchybně vystavena a odpovídá podmínkám Smlouvy a Měsíčnímu výkazu a splňuje všechny náležitosti daňového dokladu ve smyslu právních předpisů České republiky a na její vrácení, a to i opakovaně, pokud není bezchybně vystavena anebo nesplňuje všechny náležitosti daňového dokladu ve smyslu platných právních předpisů České republiky anebo k ní nebyly přiloženy požadované přílohy. Po dodání opravené Faktury začíná běžet nová lhůta splatnosti.

4.16 Dnem úhrady se rozumí den odepsání fakturované částky z účtu Objednatele složky ve prospěch účtu Poskytovatele.

4.17 Strany se dohodly a souhlasí, že Objednatel neposkytuje na plnění dle Smlouvy žádné zálohy ani závdavek a Strany uzavírají Smlouvu s přihlédnutím k tomuto ustanovení.

5. Akceptační řízení a schvalování Měsíčního výkazu

5.1 Předání a převzetí výstupů Fáze Instalace a konfigurace komunikačních center, včetně předání a převzetí dokumentů majících charakter výstupů, probíhá na základě akceptačního řízení, tj. postupným provedením testů dle testovacích scénářů, případně

jiných procesů a podepsáním předávacích a akceptačních protokolů pro jednotlivé výstupy, a to včetně veškeré příslušné dokumentace vážící se k danému výstupu Služeb, kdy podrobný popis takového postupu je popsán v tomto Článku 5.

5.2 Výstupy budou k akceptaci předány Poskytovatelem Objednateli na základě podpisu příslušného předávacího protokolu podepsaného Stranami. („**Předávací protokol**“).

5.3 Po provedení všech nezbytných činností v rámci akceptačního řízení se Objednatel i Poskytovatel zavazují podepsat příslušný akceptační protokol potvrzující výsledek akceptačního řízení („**Akceptační protokol**“).

Akceptační protokol obsahuje:

a) odkaz na tuto Smlouvu;
b) specifikaci poskytnuté Služby, resp. výstupu;
c) akceptační kritéria, jsou-li sjednána;
d) označení příslušné fáze, pod kterou předmětný výstup spadá, a
e) další informace a dokumenty nezbytné pro provedení Akceptačního řízení poskytnuté Služby.

5.4 Konkrétní akceptační kritéria pro výstupy Fáze Instalace a konfigurace komunikačních center, včetně testovacích scénářů, jsou-li dohodnuta, jsou uvedena v příslušných přílohách této Smlouvy.

V případě, že nebyla stanovena akceptační kritéria, platí, že se Strany dohodly na tom, že akceptačními kritérii budou jakékoliv podmínky a kritéria, která musí výstupy poskytování Služeb splňovat, aby dané výstupy mohly plně sloužit svému účelu a aby Infrastruktura MSpWAN byla plně funkční a poskytovala Služby Infrastruktury MSpWAN tak, jak jsou specifikována ve Smlouvě.

5.5 Výstupy Fáze Instalace a konfigurace komunikačních center, jakož i výstupy Fáze Služeb provozu, jsou způsobilé k akceptaci Objednatelem, pokud naplňují akceptační kritéria a nevykazují žádné vady, pak Objednatel vyznačí na Akceptačním protokolu „*Akceptováno*“.

V jiných případech vyznačí Objednatel na Akceptačním protokolu „*Neakceptováno*“.

5.6 Akceptační řízení je zahajováno a ukončováno podpisem následujících protokolů a uplatní se na něj následující pravidla:

(a) Je-li součástí plnění v rámci Fáze Instalace a konfigurace komunikačních center několik výstupů, pak každý z takových výstupů podléhá samostatnému akceptačnímu řízení, včetně specifických podmínek akceptačního řízení uvedených níže v tomto Článku 5;

(b) Poskytovatel a Objednatel nebo organizační složka Objednatele si dohodnou termín zahájení akceptačních testů;

(c) o předání výstupu Objednateli bude sepsán Předávací protokol, a to i v případě opakování činností v rámci akceptačního řízení v důsledku „*Neakceptováno*“ na Akceptačním protokolu;

(d) bude-li výstup nebo jeho část předávána na hmotném nosiči, bude o předání této části nebo tohoto výstupu podepsán Předávací protokol, a to i v případě opakování činností v rámci akceptačního řízení v důsledku „*Neakceptováno*“ na Akceptačním protokolu;

(e) je-li výstup akceptován vyznačením výroku „*Akceptováno*“ nasadí jej Poskytovatel do Infrastruktury MSpWAN bezodkladně poté, co jej k tomu Objednatel vyzve;

(f) posouzení výstupů Objednatelem a testy se v případě, že je na Akceptačním protokolu uveden výrok „*Neakceptováno*“ opakují, dokud nebudou splněna akceptační kritéria a neskončí akceptační řízení.

(g) V případě nutnosti opakování činností v rámci akceptačního řízení v důsledku uvedení „*Neakceptováno*“ v Akceptačním protokolu Poskytovatel Objednateli předá výstup k opětovnému provedení činností v rámci akceptačního řízení do 5 pracovních dnů (další kolo akceptačního řízení) a Poskytovatel připraví nový Akceptační protokol vztahující se k dalšímu kolu akceptačního řízení. Akceptační řízení může být vícekolové, ovšem vždy se jedná o jedno akceptační řízení;

(h) Akceptační řízení konkrétního výstupu končí a výstup se považuje za provedený a akceptovaný podpisem Akceptačního protokolu Objednatelem s uvedením „*Akceptováno*“.

(i) Po realizaci instalace a konfigurace všech komunikačních center, tzn. po podpisu Dílčích akceptačních protokolů Instalace a konfigurace pro všechna komunikační centra s výrokem Objednatele „*Akceptováno*“, Strany podepíší na závěr Fáze Instalace a konfigurace komunikačních center **Finální akceptační protokol Instalace a konfigurace komunikačních center** s výrokem Objednatele „*Akceptováno*“, čímž se tato fáze považuje za provedenou.

5.7 Akceptací v rámci Akceptačního protokolu či převzetím dle Předávacího protokolu výstupů Poskytovatele nejsou nijak dotčeny nároky Objednatele z odpovědnosti za vady. Je-li součástí plnění vytvoření dokumentu, který dále blíže specifikuje plnění v rámci dané fáze, musí být další plnění v rámci této fáze v souladu s akceptovaným dokumentem.

5.8 Lhůta k vytčení vad, resp. výhrad nemá žádný vliv na dobu trvání Záruční doby a podmínky pro uplatnění vad dle Článku 15 (*Náhrada újmy a záruka za jakost*).

5.9 Zjednodušené akceptační řízení se užije na akceptaci v rámci Fáze Služeb provozu, resp. ke schválení Měsíčních výkazů. Zjednodušené akceptační řízení bude v takovém případě probíhat pouze následovně:

(i) Měsíční výkaz slouží jako podklad k akceptaci plnění ve vztahu k vyhodnocovacímu období, kterým je 1 kalendářní měsíc („**Vyhodnocovací období**“).

(ii) Vznikne-li Objednateli nárok na smluvní pokutu za Degradaci Služeb dle Článku 16 odst. 16.3 a/nebo za Nedodržení SLA dle Článku 16 odst. 16.4, je Poskytovatel povinen v Měsíčním výkazu uvést i příslušnou smluvní pokutu (včetně specifikace, jak byla vypočtena).

(iii) Poskytovatel je povinen předat kompletní Měsíční výkaz Objednateli nejpozději do pěti (5) pracovních dní od konce Vyhodnocovacího období nebo od obdržení podkladů ze strany Objednatele, jsou-li nezbytné pro vyhotovení Měsíčního výkazu a nemůže je zajistit Poskytovatel sám, nedohodnou-li se strany jinak.

(iv) Objednatel Měsíční výkaz do pěti (5) pracovních dnů od jeho obdržení posoudí a buď ho písemně schválí nebo zašle Poskytovateli své výhrady k Měsíčnímu výkazu („**Lhůta pro schválení**“).

(v) Pokud se Objednatel ve Lhůtě pro schválení k obdrženému Měsíčnímu výkazu nevyjádří, Poskytovatel zašle Objednateli upomínku, a to nejdříve po uplynutí 5 pracovních dnů ode dne, kdy uplynula Lhůta pro schválení.

(vi) Poskytovateli vzniká nárok na úhradu Cen Služeb za dané Vyhodnocovací období až schválením příslušného Měsíčního výkazu Objednatelem.

5.10 Budou-li v rámci plnění Smlouvy předávány výstupy v listinné či elektronické podobě odlišné od Měsíčního výkazu, sepíší Strany o takovém předání Předávací protokol, případně se Strany mohou předem dohodnout, že výstup bude podléhat akceptaci a použijí se obdobně ujednání odstavců 5.1 až 7 Smlouvy.

6. Realizační tým

6.1 Poskytovatel musí poskytovat Služby po celou dobu trvání Smlouvy prostřednictvím osob uvedených v Příloze č. 5 [*Realizační tým*]. Seznam těchto osob s uvedením jejich rolí, včetně podmínek souvisejících s příslušnými rolemi a jejich kontaktních údajů, tvoří Přílohu č. 5 [*Realizační tým*] („**Realizační tým**“). Ke změně členů Realizačního týmu může dojít za podmínek uvedených dále v tomto Článku 6.

6.2 Jednotliví členové Realizačního týmu musí provádět činnosti na pozicích dle jejich odbornosti (role) uvedené v Příloze č. 5 [*Realizační tým*] a v rozsahu, který těmto rolím běžně odpovídá. Členy Realizačního týmu, jejichž prostřednictvím Poskytovatel

prokazoval kvalifikaci ve Veřejné zakázce, musí Poskytovatel využívat při plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci, ledaže dojde ke změně člena Realizačního týmu.

6.3 Využití nového člena Realizačního týmu, změnu člena Realizačního týmu nebo rozsahu jeho využití musí předem odsouhlasit Objednatel.

6.4 Při změně Realizačního týmu, musí nový člen Realizačního týmu vždy splňovat požadavky a kvalifikaci stanovené pro příslušnou roli v Zadávací dokumentaci a ve Smlouvě. Poskytovatel je povinen na žádost Objednatele kdykoliv po dobu účinnosti Smlouvy prokázat a doložit Objednateli splnění požadavků stanovených pro členy Realizačního týmu v Zadávací dokumentaci a ve Smlouvě.

6.5 Poskytovatel musí bezodkladně, nejpozději však do 5 pracovních dnů, nahradit člena Realizačního týmu na odůvodněnou žádost Objednatele v případě, že člen Realizačního týmu neplní své povinnosti podle Smlouvy nebo svou činností či nečinností způsobil Objednateli/organizační složce újmu.

6.6 Při změně Realizačního týmu není nutné uzavírat písemný dodatek ke Smlouvě. Poskytovatel po změně Realizačního týmu vypracuje a předá Objednateli v podobě elektronického dokumentu aktualizované znění Přílohy č. 5 [*Realizační tým*], čímž dojde automaticky k jejímu nahrazení novým zněním.

7. Kontaktní osoby

7.1 Strany si pro vzájemnou komunikaci ohledně Smlouvy a jejího plnění zvolily kontaktní osoby a pro některé konkrétní úkony v rámci vzájemné komunikace další osoby („**Kontaktní osoby**“), jejichž seznam je uveden v Příloze č. 7 [*Kontaktní osoby*].

7.2 Kontaktní osoby jsou za Strany oprávněny podepisovat Předávací protokoly, Akceptační protokoly a Zápis o dalším postupu. Kontaktní osoby za Objednatele jsou dále oprávněny schvalovat Žádosti o zřízení komunikačních center.

7.3 Každá Strana oznámí druhé Straně jakékoliv změny v Kontaktních osobách, případně jiných osobách stanovených v Příloze č. 7 [*Kontaktní osoby*], kontaktních údajích nebo bankovních údajích uvedených v záhlaví Smlouvy, přičemž taková změna je účinná uplynutím desátého dne po jejím skutečném doručení bez nutnosti uzavření dodatku ke Smlouvě, není-li ve Smlouvě stanoveno jinak.

7.4 Kontaktní osoby pro jednotlivé Služby na základě Požadavku budou uvedeny v příslušném Požadavku. Dojde-li ke změně Kontaktních osob v průběhu Služeb poskytovaných na základě Požadavku, oznámí tuto změnu Poskytovatel nebo Objednatel (či příslušná organizační složka) druhé Straně.

8. Účast Poddodavatelů

8.1 Poskytovatel k plnění části předmětu Smlouvy smí využít třetí osobu realizující subdodávky pro Poskytovatele v souvislosti s touto Smlouvou („**Poddodavatelé**“), s výjimkou pozice/role v Realizačním týmu „Projektový manažer“, „Solution architekt“ a „SOC/Pentest architekt“ dle Přílohy č. 5 [*Realizační tým]*, pro které možnost využití poddodavatele Objednatel vyloučil.

8.2 V Příloze č. 8 [*Poddodavatelé*] jsou uvedeni Poddodavatelé, které bude Poskytovatel využívat k poskytování Služeb.

8.3 Poskytovatel v plném rozsahu odpovídá za zapojení a činnost Poddodavatelů. Ohledně práv a povinností Poddodavatelů, jejich zaměstnanců, členů a členů statutárního orgánu se dále obdobně použijí ustanovení Smlouvy o právech a povinnostech Poskytovatele a členů Realizačního týmu podle Článku 6 (*Realizační tým*).

8.4 Využití nového Poddodavatele, změna Poddodavatele či rozsahu jeho využití musí předem písemně odsouhlasit Objednatel. V těchto případech není nutné uzavírat dodatek ke Smlouvě.

8.5 Poddodavatelé, jejichž prostřednictvím Poskytovatel prokazoval kvalifikaci ve Veřejné zakázce, je Poskytovatel povinen využívat při plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci. Poddodavatele, jimiž Poskytovatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit, pouze pokud budou nahrazeni osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu, jako nahrazovaní Poddodavatelé.

8.6 Objednatel je oprávněn uzavřít jakékoliv smlouvy s příslušnými Poddodavateli týkající se předmětu Smlouvy. Poskytovatel se zavazuje, že ve smlouvách uzavřených s Poddodavateli nevyloučí či neomezí oprávnění Poddodavatelů vstoupit do smluvních vztahů s Objednatelem, a to také včetně jakéhokoli omezení případného jednání Poddodavatelů s Objednatelem, organizačními složkami Objednatele či třetími osobami o poskytnutí takových služeb v době trvání smluvních závazkových vztahů z této Smlouvy.

9. Ochrana důvěrných informací

9.1 Poskytovatel se zavazuje zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním Smlouvy dozvěděl nebo které Objednatel (nebo organizační složka) označil za důvěrné („**Důvěrné informace**“). Důvěrné informace mohou být Poskytovatelem použity výhradně k činnostem, kterými bude zajištěno dosažení účelu této Smlouvy. Poskytovatel nesdělí či nezpřístupní žádnou z Důvěrných informací třetím osobám, nevyužije ji k vlastnímu prospěchu nebo jinak nezneužije. Povinnost mlčenlivosti a zachování Důvěrnosti informací se nevztahuje na informace, které se

staly obecně známými za předpokladu, že se tak nestalo porušením některé z povinností vyplývajících ze Smlouvy, nebo o kterých tak stanoví zákon, zpřístupnění je však možné vždy jen v nezbytném rozsahu.

9.2 Povinnost zachovávat mlčenlivost znamená zejména povinnost zdržet se jakéhokoliv jednání, kterým by důvěrné informace byly sděleny nebo zpřístupněny třetí osobě nebo by byly využity v rozporu s jejich účelem pro vlastní potřeby nebo pro potřeby třetí osoby, případně by bylo umožněno třetí osobě jakékoliv využití těchto Důvěrných informací.

9.3 Poskytovatel je povinen přijmout opatření k ochraně důvěrných informací a zajistit utajení Důvěrných informací u svých zaměstnanců nebo osob v obdobném postavení, zástupců, členů orgánů, poddodavatelů jakož i u jiných spolupracujících třetích stran, přičemž Poskytovatel nese plnou odpovědnost za porušení povinnosti mlčenlivosti ze strany těchto osob.

9.4 Povinností mlčenlivosti dle tohoto článku není dotčena povinnost dané Strany sdělit nebo zpřístupnit Důvěrné informace třetí osobě, která vyplývá z platných právních předpisů nebo z rozhodnutí orgánů veřejné moci, jakož i zpřístupnění důvěrných informací svému právnímu, účetnímu nebo daňovému poradci, kteří jsou vázáni povinností mlčenlivosti.

9.5 Povinnost zachovávat mlčenlivost trvá i po skončení tohoto smluvního vztahu.

9.6 Veškeré informace poskytnuté Objednatelem Poskytovateli se považují za Důvěrné, není-li stanoveno jinak. Veškeré informace poskytnuté Poskytovatelem Objednateli se považují za důvěrné, pouze pokud na jejich důvěrnost Poskytovatel Objednatele předem písemně upozornil a Objednatel Poskytovatel písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat. Pokud jsou Důvěrné informace Poskytovatele poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je Poskytovatel povinen upozornit Objednatele na důvěrnost takového materiálu též jejím vyznačením alespoň na titulní stránce nebo přední straně média.

9.7 Bez ohledu na výše uvedená ustanovení se za Důvěrné nepovažují informace, které:

(i) se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků některé Strany či právních předpisů,

(ii) měla daná Strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi Stranami uzavřené smlouvy o ochraně informací,

(iii) jsou výsledkem postupu, při kterém k nim Strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

(iv) po podpisu této Smlouvy poskytne Straně třetí osoba, jež není omezena v takovém nakládání s informacemi,

(v) je-li zpřístupnění informace vyžadováno zákonem či jiným právním předpisem včetně práva EU nebo závazným rozhodnutím oprávněného orgánu veřejné moci,

(vi) jsou obsažené ve Smlouvě a/nebo jsou zveřejněné na příslušných webových stránkách dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů nebo dle zákona č. 340/2015Sb, o registru smluv,

(vii) výše ceny uhrazené za plnění dle této Smlouvy v jednotlivém kalendářním roce,

(viii) Strana dá ke zpřístupnění konkrétní vlastní Důvěrné informace písemný souhlas

9.8 Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající Strany a přijímající Strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní Důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění Smlouvy, se Poskytovatel zavazuje neduplikovat žádným způsobem Důvěrné informace druhé Strany či organizačních složek, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit Smlouvu. Obě Strany se zároveň zavazují nepoužít důvěrné informace druhé Strany jinak než za účelem plnění Smlouvy.

10. Ochrana osobních údajů

10.1 Každá ze Stran prohlašuje, že bude v postavení správce zpracovávat osobní údaje fyzických osob vystupujících na straně druhé Strany jakožto subjektů údajů, a to pro účely související s plněním této Smlouvy, ochranou právních nároků a plněním právních povinností. Každá ze Stran se zavazuje o tomto informovat své zaměstnance a další fyzické osoby podílející se na plnění této Smlouvy.

10.2 Poskytovatel si je při plnění Smlouvy vědom povinností vyplývajících z platných právních předpisů týkajících se ochrany a zpracování osobních údajů, zejména ze zákona č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů („**ZZOÚ**“) a 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) („**GDPR**“). Poskytovatel je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění Smlouvy, za tímto účelem je oprávněn osobní údaje zejména ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv Poskytovatele vyplývajících ze Smlouvy, předávat zpracované osobní údaje Objednateli, osobní údaje likvidovat, vše v souladu s platnými právními předpisy týkajícími se ochrany a zpracování osobních údajů, zejména se ZZOÚ a GDPR. Zpracovává-li Poskytovatel osobní údaje, je povinen vést písemné záznamy o

činnostech zpracování a na vyžádání je poskytnout Objednateli nebo dozorovému orgánu a v případě porušení zabezpečení osobních údajů je povinen neprodleně informovat Objednatele tak, aby Objednatel mohl splnit oznamovací a/nebo ohlašovací povinnost ve lhůtách stanovených ZZOÚ a GDPR. Poskytovatel učiní v souladu s platnými právními předpisy dostatečná organizační a technická opatření zabraňující přístupu neoprávněných osob k osobním údajům.

11. Vlastnické právo a práva duševního vlastnictví

11.1 V případě, že součástí plnění Poskytovatele podle Smlouvy jsou výstupy a věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto výstupům a věcem dnem předání Objednateli (podpisem příslušného Předávacího protokolu), nestanoví-li tato Smlouva jinak. Nebezpečí škody na předaných věcech přechází na Objednatele okamžikem jejich faktického předání do dispozice Objednatele, pokud o takovém předání byl sepsán písemný záznam podepsaný oprávněnými osobami Stran.

11.2 Vznikne-li při plnění dle Smlouvy plnění, které ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, může naplňovat znaky autorského díla či být považováno za autorské dílo ve smyslu autorského zákona, poskytuje Poskytovatel Objednateli nevýhradní licenci k autorským dílům, která jsou výsledkem plnění dle Smlouvy, Poskytovatel dále poskytuje Objednateli právo dle své potřeby taková díla bez omezení upravovat a měnit (včetně provedení úprav a změn prostřednictvím třetích osob). Cena za poskytnuté licence je zohledněna v Cenách Služeb dle Článku 4 (*Cena a platební podmínky*). Objednatel není povinen licenci využít.

11.3 Strany výslovně sjednávají, že pokud Objednatel písemně nestanoví jinak, Poskytovatel není oprávněn poskytnout třetím osobám jakýkoliv výstup, který vznikne v souvislosti s poskytováním Služeb a bylo by jej možné považovat za předmět práva duševního vlastnictví.

12. Práva a povinnosti Stran

12.1 Poskytovatel se zavazuje:

(i) zajistit po celou dobu účinnosti Smlouvy dostupnost Infrastruktury MSpWAN a Služeb Infrastruktury MSpWAN minimálně 99,9 % provozní doby;

(ii) poskytovat Služby řádně a včas v souladu s pokyny a se Zadáním Objednatele a jeho organizačních složek,

(iii) hájit při poskytování Služeb oprávněné zájmy Objednatele a jeho organizačních složek,

(iv) upozorňovat Objednatele na všechny hrozící vady svého plnění či potenciální výpadky plnění, jakož i poskytovat Objednateli, případně příslušným organizačním složkám veškeré informace, které jsou pro plnění předmětu Smlouvy nezbytné,

(v) neprodleně oznámit Objednateli jakékoli překážky, které mu brání v poskytování Služeb,

(vi) postupovat při poskytování Služeb dle Smlouvy s odbornou péčí odpovídající podmínkám sjednaným ve Smlouvě,

(vii) upozornit Objednatele na potenciální rizika vzniku škod a provést včas a řádně na své náklady taková opatření, které riziko sníží nebo zcela vyloučí,

(viii) i bez pokynů Objednatele provést nutné úkony, které ač nejsou předmětem Smlouvy, budou s ohledem na nepředvídatelné okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku škody,

(ix) dodržovat bezpečnostní, hygienické, požární, organizační a další interní předpisy Objednatele a/nebo organizačních složek Objednatele, se kterými byl prokazatelně seznámen nebo které jsou všeobecně známé,

(x) na své náklady a s odbornou péčí provozovat, spravovat a udržovat veškeré technické prostředky Objednatele a/nebo organizačních složek Objednatele, které Poskytovatel převzal do užívání za účelem poskytování Služeb,

(xi) chránit při poskytování Služeb práva duševního vlastnictví Objednatele a/nebo organizačních složek Objednatele a/nebo třetích osob a zdržet se jakýchkoliv neoprávněných zásahů do práv duševního vlastnictví Objednatele, organizačních složek Objednatele nebo třetích osob,

(xii) poskytnout veškeré doklady a informace související s poskytováním Služeb ze strany Poskytovatele, které si vyžádají kontrolní orgány nebo zmocněnci pověřených orgánů. V souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů („**Zákon o finanční kontrole**“), je Poskytovatel osobou povinnou spolupůsobit při výkonu finanční kontroly. Strany se zavazují umožnit vstup do objektů a na pozemky související s poskytováním Služeb pověřeným osobám Ministerstva financí, Nejvyššího kontrolního úřadu a dalších oprávněných orgánů státní správy a Evropské unie („**Pověřené osoby**“). Poskytovatel se zavazuje zejména:

(a) poskytnout Objednateli veškeré doklady související s plněním Smlouvy, které si vyžádají Pověřené osoby, a spolupůsobit při výkonu finanční kontroly dle § 2 písm. e) Zákona o finanční kontrole, a to na náklady Poskytovatele;

(b) umožnit Pověřeným osobám kontrolu a ověření plnění Smlouvy a vytvořit Pověřeným osobám podmínky k provedení kontroly vztahujíce se k poskytování Služeb a poskytnout jim při provádění kontroly součinnost;

(c) nejméně deset (10) let od ukončení Smlouvy uchovávat originál Smlouvy, včetně jejích případných dodatků, veškeré originály účetních a dalších dokumentů souvisejících s plněním Smlouvy či vytvořených na jejím základě a zhotovit požadované informace a dokumentaci za účelem ověřování plnění dle Smlouvy. Doklady musí být uchovány způsobem uvedeným v zákoně č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a souvisejícími prováděcími právními předpisy;

(d) Poskytovatel se zavazuje zapracovat povinnosti obdobně dle tohoto odst. 12.1 písm. (xi) Smlouvy do smluv se svými Poddodavateli.

12.2 Dojde-li k přeměně společnosti Poskytovatele, ke změně vlastnické struktury společnosti Poskytovatele nebo ke změně podílu na hlasovacích právech ve společnosti Poskytovatele, v jejichž důsledku se změní ovládající osoba oproti dni uzavření Smlouvy, je Poskytovatel povinen písemně oznámit tuto skutečnost Objednateli ve lhůtě 10 pracovních dnů od účinnosti této změny.

12.3 Objednatel se zavazuje poskytovat Poskytovateli součinnost potřebnou k řádnému poskytování Služeb dle Smlouvy, zejména umožní Poskytovateli přístup do objektů za účelem poskytnutí Služeb, poskytne materiály či podklady potřebné k řádnému poskytování Služeb dle Smlouvy, lze-li poskytnutí takových materiálů či podkladů po Objednateli spravedlivě požadovat. Strany sjednávají, že Objednatel není povinen poskytnout Poskytovateli součinnost v rozsahu, v jakém si Poskytovatel může zajistit obdobné plnění, jako je předmět požadované součinnosti, jinými způsoby než prostřednictvím součinnosti Objednatele, nebo pokud je předmět požadované součinnosti součástí předmětu plnění dle Smlouvy.

12.4 V rámci součinnosti Objednatel nebo organizační složka Objednatele umožní Poskytovateli užití určených prostředků Objednatele nebo organizační složky Objednatele, a to výhradně za účelem plnění předmětu Smlouvy. Poskytovatel se zavazuje užívat tyto prostředky řádně a v souladu s provozními a bezpečnostními postupy či pokyny Objednatele a/nebo příslušné organizační složky. Poskytovatel se dále zavazuje, že nebude s těmito prostředky Objednatele nebo organizační složky nakládat nebo je používat v rozporu s touto Smlouvou nebo Požadavkem.

12.5 Strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Strany jsou povinny informovat druhou Stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění Smlouvy.

12.6 Strany se zavazují při plnění Smlouvy postupovat tak, aby nedocházelo k prodlení.

13. Povinnosti související s kybernetickou bezpečností

13.1 Poskytovatel se při poskytování Služeb zavazuje dodržovat zásady bezpečnosti informací, bezpečnostní opatření dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, povinnosti vyplývající z interních předpisů Objednatele nebo organizačních složek Objednatele, rozhodnutí či jiné pokyny Národního úřadu pro kybernetickou a informační bezpečnost v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, včetně upozorňování a zajištění hlášení kybernetických bezpečnostních incidentů a událostí, jakož i veškeré interní předpisy Objednatele týkající se této oblasti (zejména Instrukci o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti).

13.2 Kontaktní osoby Stran vzájemně komunikují v průběhu provádění Smlouvy za účelem dosažení standardů pro bezpečnost informací dle bezpečnostní dokumentace. V případě ohrožení anebo porušení bezpečnosti informací, zejména v případě výskytu kybernetické bezpečnostní události anebo incidentu, jsou Kontaktní osoby povinny vzájemně komunikovat, ihned po zjištění takových skutečností hlásit jejich výskyt druhé Straně a společně podnikat kroky k zajištění obnovení bezpečnosti informací.

13.3 Poskytovateli nenáleží za plnění povinností souvisejících s bezpečností informací ve smyslu tohoto Článku 13 (*Povinnosti související s kybernetickou bezpečností*) odměna, resp. taková odměna je součástí Ceny Služeb.

14. Pojištění

14.1 Poskytovatel se zavazuje do 14 dnů od účinnosti Smlouvy předložit Objednateli a udržovat v platnosti po celou dobu trvání závazkových právních vztahů založených touto Smlouvou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou v souvislosti s výkonem činností, které jsou předmětem Smlouvy s limitem pojistného plnění nejméně ve výši 200 000 000 Kč (slovy: dvě stě milionů korun českých), a to ze všech pojistných událostí vzniklých v jednom pojišťovacím roce v souvislosti s touto Smlouvou. Ve vztahu k pojištění dle tohoto Článku 14 (*Pojištění*)

se Poskytovatel zavazuje zajistit, že v případě vzniku pojistné události bude pojistné plnění placeno přímo Objednateli.

14.2 Poskytovatel nemůže snížit výši pojistného krytí nebo podstatným způsobem s negativními důsledky pro Objednatele změnit podmínky pojistné smlouvy dle odstavce 14.1 bez předchozího písemného souhlasu Objednatele.

14.3 Poskytovatel kdykoliv v průběhu trvání Smlouvy na požádání Objednatele předloží platnou a účinnou pojistnou smlouvu dle odst. 14.1, nebo pojistku ve smyslu § 2775 Občanského zákoníku či jiný pojistný certifikát, a to vždy nejpozději do 7 dnů ode dne doručení žádosti Objednatele.

14.4 Jestliže Poskytovatel nebude udržovat pojištění dle tohoto Článku 14 (*Pojištění*) v platnosti nebo nepředloží Objednateli včas doklady dle odst. 14.3, může Objednatel v takovém případě svým jménem sjednat a udržovat pojištění ve stejném rozsahu a pokrývající stejná rizika jako pojištění, které měl zajistit Poskytovatel, platit pojistné a započíst platbu za pojistné vůči jakýmkoliv peněžním nárokům Poskytovatele vyplývajícím ze Smlouvy.

14.5 Ustanovení odstavce 14.4 není na újmu jiným nárokům a oprávněním Objednatele stanoveným ve Smlouvě.

14.6 Náklady Poskytovatele na pojištění dle tohoto Článku 14 (*Pojištění*) jsou zahrnuty v Cenách Služeb. Uvedená částka pojistného plnění dle odst. 14.1 se vztahuje na újmu včetně případných nákladů řízení spojených s jejím uplatněním.

15. Náhrada újmy a záruka za jakost

15.1 Každá ze Stran nahradí způsobenou újmu v rámci platných právních předpisů a této Smlouvy. Obě Strany vyvinou maximální úsilí k předcházení újem a k minimalizaci vzniklých újem.

15.2 Poskytovatel poskytující v souladu se svým prohlášením v Preambuli Smlouvy Služby jako odborník dle § 2950 Občanského zákoníku nahradí v plném rozsahu škodu, způsobí-li ji v rámci poskytování Služeb neúplnou nebo nesprávnou informací nebo radou danou v záležitosti jeho vědění nebo dovedností.

15.3 Žádná ze Stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Strany. V případě, že jedna ze Stran poskytla druhé Straně chybné zadání a příslušná Strana s ohledem na svou povinnost poskytovat plnění s odbornou péčí mohla a měla chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání příslušná Strana druhou Stranu písemně upozornila a druhá Strana trvala na původním zadání.

15.4 Strany se zavazují upozornit druhou Stranu bez zbytečného odkladu na vznik mimořádné nepředvídatelné a nepřekonatelné překážky vzniklé nezávisle na jejich vůli bránící řádnému plnění Smlouvy (§ 2913 Občanského zákoníku). Strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání předmětných překážek.

15.5 Případná náhrada škody bude zaplacena v měně platné na území České republiky, přičemž pro propočet na tuto měnu je rozhodný kurs České národní banky ke dni vzniku škody.

15.6 Poskytovatel poskytuje Objednateli záruku za jakost svých výstupů po dobu 2 let ode dne akceptace výstupu nebo ode dne schválení příslušného Měsíčního výkazu („**Záruční doba**“). Poskytovatel odpovídá za vady zjevné, skryté i právní, které mají výstupy v době jejich předání Objednateli a za ty, které se vyskytnou v Záruční době. Poskytovatel se zavazuje vady bezplatně odstranit do 5 kalendářních dnů od jejich nahlášení Objednatelem/organizační složkou.

16. Smluvní pokuty a úrok z prodlení

16.1 Je-li Objednatel v prodlení s úhradou Ceny Služeb dle Článku 4 (*Cena a platební podmínky*), je Poskytovatel oprávněn požadovat na Objednateli úrok z prodlení z neuhrazené dlužné částky podle konkrétní Faktury za každý den prodlení ve výši stanovené zvláštním právním předpisem, kterým se stanoví výše úroků z prodlení (nařízení vlády č. 351/2013 Sb.).

16.2 Nedodrží-li Poskytovatel lhůtu dle Článku 2 odst. 2.34 pro dokončení Fáze Instalace a konfigurace komunikačních center a pro zprovoznění všech komunikačních center v Implementačních lokalitách dle Přílohy č. 4 [*Seznam a kategorizace Implementačních lokalit*] vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 5 000,- Kč za každý započatý den prodlení a 10 000,- Kč za každé nezprovozněné komunikační centrum.

16.3 Nedodrží-li Poskytovatel dostupnost Infrastruktury MSpWAN nebo Služeb Infrastruktury MSpWAN dle Smlouvy („**Degradace Služeb**“), vzniká Objednateli nárok na zaplacení smluvní pokuty.

Pro výpočet smluvních pokut budou použity hodinové sazby za Degradaci Služeb dle následující tabulky:

Hodinová sazba za Degradaci Služeb	**Kategorie komunikačního centra**
1 000,- Kč/započatou hodinu	Malé komunikační centrum
2 000,- Kč/započatou hodinu	Střední komunikační centrum

5 000,- Kč/započatou hodinu	Velké komunikační centrum
50 000,- Kč/započatou hodinu	Hlavní komunikační centrum

V případě Degradace Služeb Hlavního komunikačního centra, která způsobí celkovou Degradaci Služeb Infrastruktury MSpWAN, se počítají sankce pouze za Degradaci Služeb Hlavního komunikačního centra.

Celková smluvní pokuta za Degradaci služeb je součtem Dílčích smluvních pokut za Degradaci Služeb pro jednotlivé kategorie komunikačních center.

Dílčí smluvní pokuta pro danou kategorii komunikačního centra je součinem počtu nefunkčních komunikačních center dané kategorie (hlavní/velké/střední/malé), příslušné Sazby za Degradaci služeb a doby nefunkčnosti v hodinách.

16.4 Nedodrží-li Poskytovatel úroveň servisních služeb (SLA) definovanou v Příloze č. 2 [*Úroveň servisních služeb (SLA)*] („**Nedodržení SLA**“), vzniká Objednateli nárok na zaplacení smluvní pokuty.

Smluvní pokuty za Nedodržení SLA jsou určeny jako součin Sazby za Nedodržení SLA a doby Nedodržení SLA v hodinách.

Sazby za Nedodržení SLA jsou určené dle následující tabulky:

Sazba za Nedodržení SLA	**Důvod Nedodržení SLA**
1 000,- Kč/započatou hodinu	Nedodržení Provozní doby ServiceDesk *(nedodržení 24x7)*
	Nedodržení dostupnosti ServiceDesk *(nedodržení dostupnosti 99,6%)*
	Nedodržení Reakční doby na nahlášení incidentu/požadavku *(nedodržení RESPONSE TIME)*
	Nedodržení doby vyřešení incidentu s Prioritou P3 (střední) *(nedodržen FIX TIME 12 hodin)*
	Nedodržení doby vyřešení incidentu s Prioritou P4 (vysoká) *(nedodržen FIX TIME 24 hodin)*

Sazba za Nedodržení SLA	**Důvod Nedodržení SLA**
	Nedodržení doby vyřešení požadavku s Prioritou P3 (střední) *(nedodržen FIX TIME 24 hodin)*
	Nedodržení doby vyřešení požadavku s Prioritou P4 (nízká) *(nedodržen FIX TIME 48 hodin)*
5 000,- Kč/započatou hodinu	Nedodržení doby vyřešení incidentu nebo požadavku s Prioritou P1 (urgentní) *(nedodržen FIX TIME 4 hodiny)*
2 000,- Kč/započatou hodinu	Nedodržení doby vyřešení incidentu s Prioritou P2 (vysoká) *(nedodržen FIX TIME 8 hodin)*
	Nedodržení doby vyřešení požadavku s Prioritou P2 (vysoká) *(nedodržen FIX TIME 12 hodin)*

16.5 Pokud by došlo k nesprávnému postupu Objednatele či organizační složky z důvodu opomenutí či chyby Poskytovatele při poskytování Služeb, je Objednatel oprávněn požadovat po Poskytovateli uhrazení smluvní pokuty ve výši rovnající se sankci uložené rozhodnutím příslušného orgánu státní správy nebo jiným orgánem veřejné moci.

16.6 Poruší-li Poskytovatel povinnost uvedenou v Článku 1 odst. 1.3 bod (iii) týkající se udržování, aktualizace a zpřístupnění Dokumentace Objednateli, včetně zpřístupnění přístupových údajů s právem čtení (read-only), vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 5 000 Kč za každé zjištěné porušení této povinnosti.

16.7 V každém jednotlivém případě porušení ochrany Důvěrných informací podle Článku 9 (*Ochrana důvěrných informací*) vzniká druhé Straně právo požadovat zaplacení smluvní pokuty ve výši 500 000,- Kč.

16.8 Pokud Poskytovatel poruší povinnost chránit Osobní údaje v souladu s Článkem 10 (*Ochrana osobních údajů*), vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 500 000,- Kč za každé zjištěné porušení této povinnosti.

16.9 Pokud Poskytovatel poruší povinnost udělit Objednateli oprávnění v rozsahu dle Článku 11 (*Vlastnické právo a práva duševního vlastnictví*), vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 100 000,- Kč za každé zjištěné porušení této povinnosti.

16.10 Pokud Poskytovatel poruší povinnost udržovat v platnosti pojištění dle Článku 14 (*Pojištění)*, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 100 000,- Kč za každé zjištěné porušení této povinnosti.

16.11 Pokud je Poskytovatel v prodlení s plněním povinnosti oznámit Objednateli změnu skutečností dle Článku 12 odst. 12.2, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 10 000,- Kč za každý den prodlení.

16.12 Poruší-li Poskytovatel některou z povinností týkajících se Článku 6 (*Realizační tým)* vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 100 000,- Kč za každé zjištěné porušení této povinnosti.

16.13 Pokud Poskytovatel poruší povinnost zachovávat bezpečnost informací dle Článku 13 (*Povinnosti související s kybernetickou bezpečností*), vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši dvojnásobku částky sankce případně uložené z tohoto důvodu Objednateli ze strany příslušného správního orgánu. Objednatel je však, za předpokladu, že mu k tomu Poskytovatel poskytne nezbytnou součinnost, povinen uplatnit v příslušných řízeních veškeré přiměřené námitky, které mohl uplatnit ve svém zájmu, a v rámci řízení je povinen řádně hájit svá práva.

16.14 V případě porušení smluvní povinnosti, mimo zvláštních ustanovení uvedených v tomto článku Smlouvy, je Objednatel oprávněn požadovat smluvní pokutu ve výši 10 000,- Kč za každý jednotlivý případ porušení povinnosti stanovené touto Smlouvou, není-li v tomto článku stanovena specifická smluvní pokuta.

16.15 Ujednáním o smluvních pokutách dle předchozích odstavců tohoto Článku 16 není dotčeno právo Objednatele na náhradu škody, a to i ve výši přesahující sjednanou smluvní pokutu. Strany se dohodly, že ustanovení § 2050 Občanského zákoníku se nepoužije.

16.16 Splatnost smluvních pokut činí deset (10) dnů ode dne doručení výzvy k její úhradě Poskytovateli. Výjimku tvoří smluvní pokuty dle odst. 16.3 a odst. 16.4 tohoto Článku, u kterých bude postupováno v souladu s Článkem 4 odst. 4.13 a s Článkem 5 odst. 5.9.

16.17 Objednatel je oprávněn započíst pohledávku na úhradu smluvní pokuty vůči pohledávce Poskytovatele na úhradu Ceny Služeb, s čímž Poskytovatel výslovně souhlasí.

16.18 Smluvní pokuta nemá vliv na uplatnění náhrady újmy ani na odpovědnost za vady.

17. Trvání a ukončení Smlouvy

17.1 Tato Smlouva se uzavírá na dobu určitou, přičemž Smlouva nabývá účinnosti dnem uveřejnění v registru smluv a skončí uplynutím 10 let (120 měsíců) od 1. dne následujícího měsíce po dni podepsání Finálního akceptačního protokolu Instalace a konfigurace komunikačních center s výrokem Objednatele „*Akceptováno*“.

17.2 Kromě uplynutí doby dle odst. 17.1 tohoto Článku lze Smlouvu ukončit písemnou dohodou Stran nebo odstoupením od Smlouvy.

17.3 Strany mohou Smlouvu ukončit písemnou dohodou. V této dohodě bude sjednán způsob vypořádání vzájemných nároků.

17.4 Odstoupit od Smlouvy může kterákoli ze Stran v případě, že druhá Strana poruší smluvní povinnosti podstatným způsobem. Odstoupení od Smlouvy doručí odstupující Strana druhé Straně. Odstoupení od Smlouvy je účinné a Smlouva zaniká dnem doručení písemného odstoupení druhé Straně, není-li v odstoupení stanoveno pozdější datum. Od Smlouvy je možné odstoupit pouze s účinky *ex nunc* (do budoucna).

17.5 Strany se dohodly na vyloučení použití § 1978 odst. 2 Občanského zákoníku, který stanoví, že marné uplynutí dodatečné lhůty stanovené k plnění má za následek odstoupení od Smlouvy bez dalšího.

17.6 Odstoupení od Smlouvy Objednatelem. Objednatel je oprávněn odstoupit od Smlouvy v případě jejího podstatného porušení ze strany Poskytovatele, zejména, nikoliv však výlučně, jestliže:

(a) Poskytovatel je v prodlení s plněním dle této Smlouvy o více než 15 dnů a nezjedná nápravu ani do 15 dnů od doručení písemného oznámení Objednatele o takovém prodlení;

(b) Poskytovatel poruší Smlouvu jiným nepodstatným způsobem a ve lhůtě 15 dnů ode dne obdržení písemné výzvy Objednatele k nápravě toto své porušení nenapraví;

(c) Poskytovatel poruší podstatným způsobem povinnosti

i) mlčenlivosti o Důvěrných informacích;
ii) pro nakládání s Osobními údaji;
iii) vyplývající mu z požadavků na kybernetickou bezpečnost.

(d) Poskytovatel podá insolvenční návrh jako dlužník ve smyslu § 98 zák. č. 182/2006 Sb., insolvenční zákon („**Insolvenční zákon**“), nebo insolvenční soud nerozhodne o insolvenčním návrhu na Poskytovatele do šesti (6) měsíců od zahájení insolvenčního řízení, nebo insolvenční soud vydá rozhodnutí o úpadku Poskytovatele ve smyslu § 136 Insolvenčního zákona,

(e) je přijato rozhodnutí o povinném nebo dobrovolném zrušení Poskytovatele (vyjma případů sloučení nebo splynutí);

(f) okolnost vylučující povinnost k náhradě újmy Poskytovatele trvá déle než třicet (30) dnů;

(g) Poskytovatel či Poddodavatel je nebo se v průběhu účinnosti Smlouvy stane osobou, na kterou se vztahuje zákaz zadání veřejné zakázky dle § 48a ZZVZ;

(h) se prokáže, že zájmy osob ve smyslu § 44 odst. 2 písm. a) a b) ZZVZ získat osobní výhodu nebo snížit majetkový nebo jiný prospěch Objednatele, ohrožují jejich nestrannost nebo nezávislost v souvislosti se zadávacím řízením, nebo

(i) dojde k přeměně společnosti Poskytovatele, změně vlastnické struktury společnosti Poskytovatele či změně podílu na hlasovacích právech ve společnosti Poskytovatele dle Článku 12 odst. 12.2 Smlouvy.

17.7 Odstoupení od Smlouvy Poskytovatelem. Poskytovatel je oprávněn odstoupit od Smlouvy pouze v případě, že:

(a) Objednatel je déle než 30 dnů v prodlení se zaplacením Cen Služeb a toto své porušení nenapraví do 15 dnů ode dne obdržení písemné výzvy k nápravě a následně ani v dodatečné lhůtě 15 dnů ode dne obdržení druhé písemné výzvy k nápravě, v níž bude Poskytovatelem výslovně upozorněn na možnost Poskytovatele odstoupit od Smlouvy;

(b) Objednatel poruší jinak přímo Smlouvu podstatným způsobem, toto své porušení nenapraví do 30 dnů ode dne obdržení písemné výzvy k nápravě a následně ani v dodatečné lhůtě patnácti 15 dnů ode dne obdržení druhé písemné výzvy k nápravě, v níž bude Poskytovatelem výslovně upozorněn na možnost Poskytovatele odstoupit od Smlouvy; nebo

(c) okolnost vylučující povinnost k náhradě újmy Objednatele trvá déle než 30 dnů.

17.8 Při předčasném ukončení Smlouvy, budou vzájemné závazky a pohledávky vypořádány písemnou dohodou Stran.

17.9 V případě, že při ukončení Smlouvy vznikne Objednateli potřeba výstupů Služeb, implementované Infrastruktury MSpWAN nebo její části, technických prostředků nezbytných pro zajištění funkčnosti Infrastruktury MSpWAN a Objednatel bude tento majetek potřebovat k plnění funkcí státu nebo jiných úkolů v rámci své působnosti nebo stanoveného předmětu činnosti, je Objednatel oprávněn učinit volbu, zda za podmínek zákona č. 219/2000Sb., o majetku České republiky a jejím vystupování v právních vztazích, ve znění pozdějších předpisů, uzavře s Poskytovatelem smlouvu o převodu takového majetku, a to za cenu stanovenou znaleckým posudkem a s ohledem na účelnost a hospodárnost takového postupu.

17.10 Ukončením Smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, náhrady újmy, povinnosti mlčenlivosti a ochrany důvěrných informací a ochrany osobních údajů a ustanovení týkající se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po skončení účinnosti Smlouvy.

18. Ostatní ujednání

18.1 Smlouva se řídí právním řádem České republiky. Nestanoví-li některý právní předpis jinak, budou veškeré spory mezi Stranami vzniklé ze Smlouvy nebo v souvislosti s ní řešeny před věcně a místně příslušným soudem České republiky.

18.2 Poskytovatel je podle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

18.3 Objednatel je oprávněn uveřejnit na svých webových stránkách a v registru smluv celý text Smlouvy, vše za předpokladu, nebrání-li uveřejnění zvláštní právní předpis.

18.4 Poskytovatel přebírá podle § 1765 Občanského zákoníku riziko změny okolností v souvislosti s plněním této Smlouvy.

18.5 Strany souhlasně prohlašují, že Smlouva není smlouvou uzavřenou adhezním způsobem ve smyslu ustanovení § 1798 a násl. Občanského zákoníku. Ustanovení § 1799 a § 1800 Občanského zákoníku se nepoužijí.

18.6 Strany vylučují použití všeobecných obchodních podmínek či obdobného dokumentu Poskytovatele.

19. Rozhodné právo a řešení sporů

19.1 Smlouva se řídí a bude vykládána v souladu s právním řádem České republiky, zejména Občanským zákoníkem. Strany se dohodly, že obchodní zvyklosti nemají přednost před žádnými ustanoveními zákona, a to ani před ustanoveními zákona, jež nemají donucující účinky.

19.2 Strany se zavazují řešit veškeré spory, které mezi nimi mohou vzniknout v souvislosti s prováděním nebo výkladem Smlouvy, jednáním a vzájemnou dohodou.

19.3 Dojde-li mezi Stranami ke sporu souvisejícího s předmětem plnění dle Smlouvy, který má, či by mohl mít dopad na poskytování Služeb, uskuteční Strany nejpozději do 10 pracovních dnů od vzniku sporu osobní schůzku osob oprávněných za Strany k podpisu této Smlouvy, a to za účelem vyřešení vzniklého sporu („**Eskalační proces**“).

19.4 Pokud se nepodaří vyřešit předmětný spor, bude takový spor předložen jednou ze Stran věcně a místně příslušnému soudu. Strany si tímto sjednávají místní příslušnost obecného soudu Objednatele.

20. Závěrečná ujednání

20.1 Veškeré změny a doplňky Smlouvy musí být učiněny písemně ve formě číslovaného dodatku ke Smlouvě, podepsaného k tomu oprávněnými zástupci obou Stran. Výjimky z ujednání předchozí věty tvoří:

(a) úpravy počtu a kategorizace Implementačních lokalit, při kterých se uplatní postup dle Článku 2 odstavce 2.2 Smlouvy;

(b) úpravy Přílohy č. 5 [*Realizační tým*], při kterých se uplatní postup dle Článku 6 odst. 6.3 a 6.56 Smlouvy;

(c) úpravy Přílohy č. 7 [*Kontaktní osoby*], při kterých se uplatní postup dle Článku 7 odst. 7.3 Smlouvy;

(d) využití nového Poddodavatele, kdy je nutné postupovat dle Článku 8 odst. 8.44 Smlouvy.

20.2 Strany prohlašují, že Smlouva obsahuje veškerý projev jejich shodné vůle a mimo ni neexistují žádná ujednání v jiné než písemné formě, která by ji doplňovala, měnila nebo mohla mít význam při jejím výkladu a že se tedy žádná ze Stran nespoléhá na prohlášení druhé Strany, které není uvedeno ve Smlouvě, jejích přílohách či dodatcích. Tím není dotčen význam komunikace Stran, včetně pokynů Objednatele.

20.3 Smlouvě je podepsána v listinné podobě nebo elektronicky. Je-li Smlouva podepsána v listinné podobě, je vyhotovena ve čtyřech (4) výtiscích s platností originálu, z nichž každá Strana obdrží po dvou (2) vyhotoveních. Je-li Smlouva podepsána elektronicky, je podepsána pomocí kvalifikovaného elektronického podpisu.

20.4 Smlouva nabývá platnosti dnem podpisu oběma Stranami a účinnosti dnem uveřejnění v registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel.

20.5 Stane-li se některé ujednání Smlouvy neplatným, zdánlivým či neúčinným, nemá tato skutečnost vliv na ostatní ujednání Smlouvy, která zůstávají platná a účinná. Strany se v tomto případě zavazují písemnou dohodou nahradit ujednání, které bylo shledáno neplatným, zdánlivým či neúčinným novým ujednáním, které po obsahové stránce nejlépe odpovídá zamýšlenému účelu původního ujednání. Do té doby platí odpovídající úprava obecně závazných právních předpisů České republiky.

20.6 Vyskytnou-li se události, které jedné nebo oběma Stranám částečně nebo úplně znemožní plnění jejich povinností podle Smlouvy, jsou Strany povinny se o tomto bez zbytečného odkladu informovat a společně podniknout kroky k jejich překonání.

20.7 Strany prohlašují, že Smlouva byla sjednána na základě jejich pravé, vážné a svobodné vůle, že si její obsah přečetly, bezvýhradně s ním souhlasí, považují jej za zcela určitý a srozumitelný, což níže stvrzují svými podpisy.

20.8 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1: Technická specifikace

Příloha č. 1A: Hlavní komunikační centrum

Příloha č. 1B: Velké komunikační centrum

Příloha č. 1C: Střední komunikační centrum

Příloha č. 1D: Malé komunikační centrum

Příloha č. 2: Úroveň servisních služeb (SLA)

Příloha č. 3: Žádost o zřízení komunikačního centra

Příloha č. 4: Seznam a kategorizace Implementačních lokalit

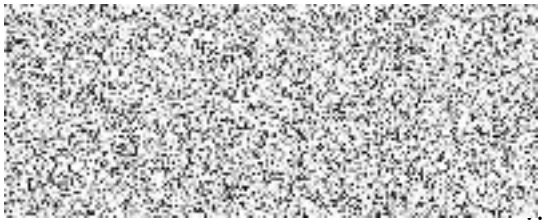
Příloha č. 5: Realizační tým

Příloha č. 6: Vzor měsíčního výkazu

Příloha č. 7: Kontaktní osoby

Příloha č. 8: Poddodavatelé

V Praze dne



……

Česká republika – Ministerstvo spravedlnosti
Ing. Bc. Radomír Daňhel MBA, LL.M.
náměstek člena vlády
pověřený v oblasti ekonomické a správní

V Praze dne

……..

ALEF NULA, a.s.
Ing. Milan Zinek
předseda představenstva

Příloha č. 1 – Technická specifikace

1 Základní pojmy a definice

- **Infrastruktura MSpWAN** – Soubor technických zařízení a software vytvářející pro resort Objednatele dedikovanou WAN (Wide Area Network) infrastrukturu.

- **Služby Infrastruktury MSpWAN** – služby a procesy zajišťující dlouhodobé užívání kapacitní, bezpečné, vysoce spolehlivé a technologicky relevantní Infrastruktury MSpWAN Objednatelem, organizačními složkami Objednatele nebo třetími stranami.

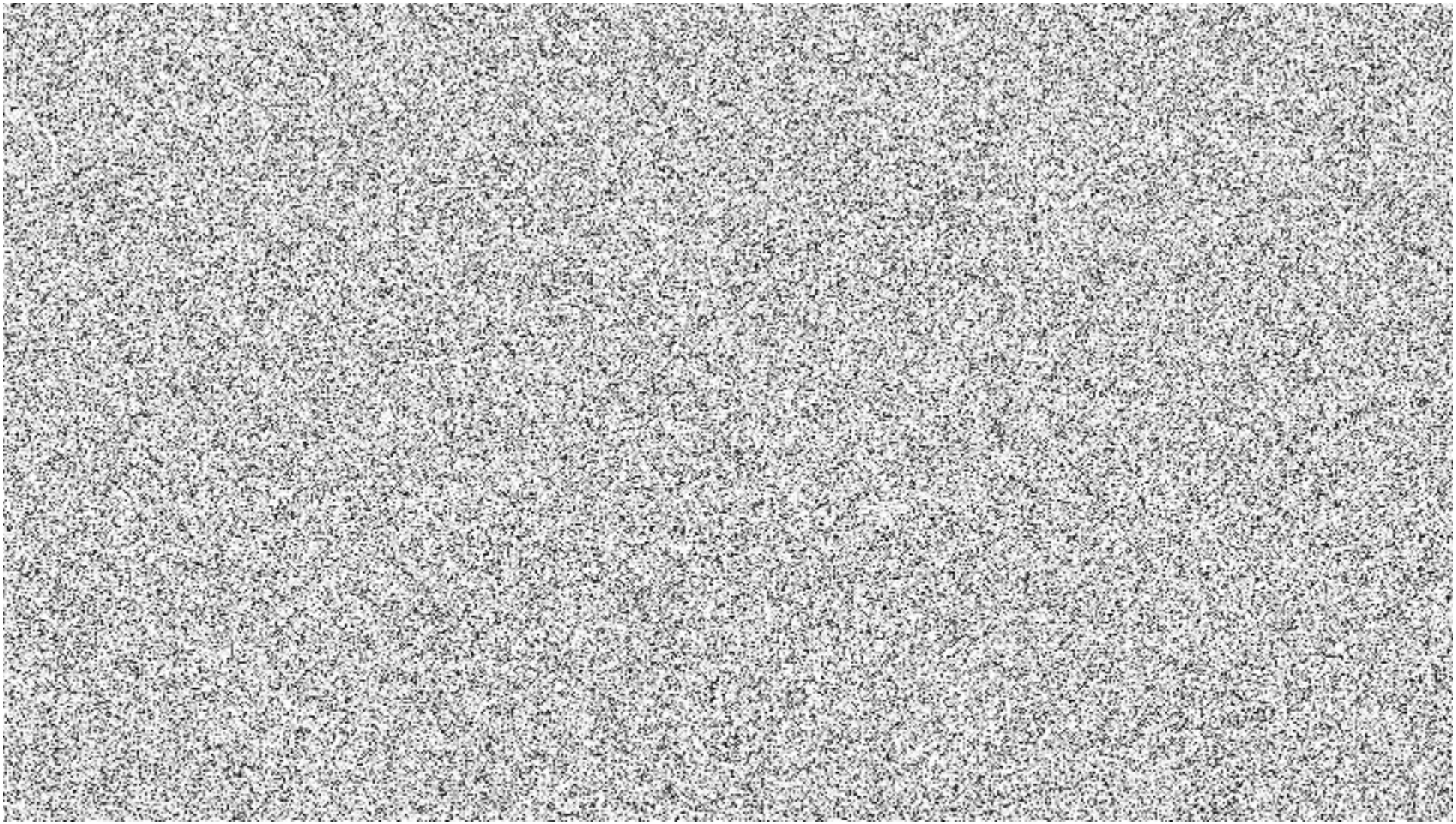
- **Hlavní komunikační centrum** – Soubor technických prostředků v lokalitách Objednatele, které tvoří základ a nejdůležitější součást Infrastruktury MSpWAN.

- **Malé/Střední/Velké komunikační centrum** – Soubor technických prostředků tvořících Infrastrukturu MSpWAN umístěných v lokalitě, kde působí organizační složky Objednatele.

- **Implementační lokalita** – Fyzické místo určené adresou, v němž je umístěné komunikační centrum. Seznam a specifikace Implementačních lokalit je uveden v Příloze č. 4 [*Seznam a kategorizace Implementačních lokalit*].

- **KIVS (komunikační infrastruktura veřejné správy)** – Síťová infrastruktura, kterou zajišťuje prostřednictvím jiných poskytovatelů dle vlastních smluv s nimi Objednatel a která umožňuje datové přenosy mezi Komunikačními centry navzájem.

2 Infrastruktura MSpWAN



Infrastrukturu MSpWAN tvoří:

- **Hlavní komunikační centra** v celkovém počtu 2 kusy. Podrobný popis je v Příloze č. 1A [Hlavní komunikační centrum].

- **Velká komunikační centra**, kterých je ke dni nabytí účinnosti Smlouvy 25 kusů. Podrobný popis je v Příloze č. 1B [Velké komunikační centrum].

- **Střední komunikační centra**, kterých je ke dni nabytí účinnosti Smlouvy 60 kusů. Podrobný popis je v Příloze č. 1C [Střední komunikační centrum].

- **Malá komunikační centra**, kterých je ke dni nabytí účinnosti Smlouvy 175 kusů. Podrobný popis je v Příloze č. 1D – [Malé komunikační centrum].

Objednatel výslovně upozorňuje, že s výjimkou počtu Hlavních komunikačních center, se počet komunikačních center může v čase měnit.

3 Služby Infrastruktury MSpWAN

Služby Infrastruktury MSpWAN jsou provozovány za účelem zajištění kapacitní, bezpečné, vysoce spolehlivé a technologicky relevantní konektivity mezi komunikačními centry využívanými Objednatelem, organizačními složkami nebo třetími stranami a umožnění vysoké míry interoperability mezi nimi.

Základní Služby Infrastruktury MSpWAN:

- Centrální automatizovaný management Infrastruktury MSpWAN

- Bezpečnostní dohled nad Infrastrukturou MSpWAN

- Provoz Infrastruktury MSpWAN.

3.1 Výpočetní prostředí pro Služby Infrastruktury MSpWAN

Pro zajištění poskytování Služeb Infrastruktury MSpWAN je nutné vybudovat a udržovat výpočetní prostředí v datových centrech Objednatele.

Identifikace výpočetního prostředí:

Výrobce	**Cisco**
Obchodní název	**Cisco Compute Hyperconverged HCIAF240cM7**
Model	**HCI AF C240M7N**
Part-number	**HCIAF240C-M7SN**

Požadavky na výpočetní prostředí

Požadovaná funkcionalita/vlastnost	
Dva hyperkonvergované clustery sestávající každý z minimálně 4 bloků pro zajištění vysoké dostupnosti. Clustery budou provozovány ve dvou vzdálených Data Centrech	
Cluster v každé lokalitě musí poskytnout virtuální prostředky pro provoz centrální správy • 250 routerů; • 250 Firewallů a • 250 Switchů. a musí být dimenzován v dostatečné rychlosti a kvalitě dle best practice výrobců jednotlivých technologií a požadované retenci logů minimálně jeden měsíc při kompletním logování provozu.	
Hardware konfigurace jednoho clusteru	minimálně 240 procesorových jader minimálně 2,0 TB RAM minimálně 480TB úložiště z čehož minimálně 150TB z této kapacity musí být tvořeno poolem SSD nebo NVMe disků
Pro potřeby Clusteru a virtualizační platformy je vyžadováno připojení do infrastruktury MSp	minimálně 10x100Gbe QSFP28 konektivity v každém z obou datacenter
Maximální výška pro montáž Clusteru per Data Centrum MSp je 10U	
Clustery musí umožňovat mezi sebou synchronní replikaci dat pro maximalizaci dostupnosti provozované služby centrální správy routerů, firewallů, switchů	
Data musí být na úložiště ukládána v šifrované podobě	
Software i firmware bloků clusteru musí být možné aktualizovat za provozu bez negativního dopadu na provozované systémy.	
Řešení musí podporovat mikrosegmentaci	
Dohled clusterů bude realizován dohledovým systémem Objednatele.	

3.2 Centrální automatizovaný management Infrastruktury MSpWAN

Centrální automatizovaný management Infrastruktury MSpWAN je realizován prostřednictvím

- Centrálního automatizovaného managementu routerů a SD-WAN Fabric
- Centrálního automatizovaného managementu firewallů
- Centrálního automatizovaného managementu Switchů.

Specifikace Centrálního automatizovaného managementu routerů a SD-WAN Fabric

Identifikace Centrálního automatizovaného managementu routerů a SD WAN Fabric:

Výrobce	**Cisco**
Obchodní název	**Cisco SD-WAN Controller**

Požadovaná funkcionalita/vlastnost
Zařízení typu centrální správa Routerů ve formě virtuální appliance umístěné ve virtualizačním prostředí MSpWAN - On-Premis
Minimálně 250 centrálně spravovaných Routerů včetně všech jejich funkcionalit a všech potřebných licencí pro centrální správu
SD-WAN fabric je založena na architektuře Software Defined Networks s plně oddělenou řídící vrstvou (control plane) a datovou vrstvou (data plane)
SD-WAN fabric umožňuje centralizovanou správu a monitoring jednotlivých prvků prostřednictvím grafického uživatelského rozhraní centrální management konzole
Veškeré řídící prvky SD-WAN fabric musí být nasazeny v privátním datovém centru zákazníka
Řízení provozu v rámci SD-WAN fabric infrastruktury je realizováno prostřednictvím předem definovaných síťových politik
Veškeré síťové a bezpečnostní politiky (Firewall, IPS, URL filtrace apod.) jsou definovány prostřednictvím centrální management konzole pomocí předdefinovaných workflows
Vzájemná autentizace všech prvků SD-WAN fabric infrastruktury prostřednictvím X.509 certifikátů
Připojování jednotlivých prvků do SD-WAN fabric je ověřováno vůči předem definovanému explicitnímu seznamu prvků tvořících SD-WAN fabric, tzv. white-listu
SD-WAN fabric umožňuje Zero Touch Provisioning data plane infrastruktury
GUI rozhraní centrální management konzole poskytuje detailní přehled o výkonnosti a stavu celé SD-WAN fabric infrastruktury včetně monitorování stavu jednotlivých zařízení (využití CPU, DRAM paměti, jednotlivých síťových rozhraní atd.)
Centrální management konzole zjišťuje kompletní SW image management pro všechny prvky SD-WAN fabric
Centrální management konzole umožňuje provádět SW image upgrade pro jednotlivé prvky SD-WAN fabric v předem plánovaném čase
Centrální management konzole umožnuje spouštět na jednotlivých prvcích SD-WAN fabric troubleshooting nástroje jako je ping a traceroute ato jak pro protokol IPv4, tak i pro protokol IPv6
Centrální management konzole obsahuje nástroje umožňující simulaci datových toků mezi koncovými prvky SD-WAN fabric
SD-WAN fabric podporuje různé transportní infrastruktury jako např. MPLS VPN, Broadband Internet, 5G, LTE, satelitní spoje apod.
SD-WAN fabric podporuje transportní infrastruktury využívající jak protokol IPv4, tak i protokol IPv6
Řídící komunikace mezi jednotlivými prvky SD-WAN fabric je možné zabezpečit prostřednictvím technologie TLS 1.3

Požadovaná funkcionalita/vlastnost
Veškerá řídící komunikace mezi jednotlivými prvky SD-WAN fabric je šifrovaná prostřednictvím algoritmu AES-GCM-256
SD-WAN fabric využívá pro šifrování datového provozu mezi jednotlivými lokalitam WAN sítě protokol IPSec s šifrovacím algoritmem AES-GCM-256
Vzájemná výměna IPSec šifrovacích klíčů mezi jednotlivými prvky SD-WAN fabric probíhá přes oddělený zabezpečený komunikační kanál
SD-WAN fabric umožňuje zcela automatické vytvoření full-mesh topologie IPSec spojení mezi jednotlivými lokalitami
SD-WAN fabric umožňuje vytvoření Hub-Spoke topologie IPSec spojení mezi jednotlivými lokalitami
SD-WAN fabric podporuje dynamické (On Demand) vytváření šifrovaných spojení mezi vzdálenými lokalitami v případě , že je potřeba přenést datový provoz přímo mezi vzdálenými lokalitami
SD-WAN fabric umožňuje vytváření hierarchických topologií, např. umožňuje aplikovat full-mesh topologii pro vzájemné propojení regionálních center a současně aplikovat hub-spoke topologii pro propojení lokalit v rámci jednotlivých regionů
SD-WAN fabric umožňuje segmentovat provoz koncových uživatelů, zařízení a aplikací do oddělených virtuálních privátních sítí (VPN) včetně plné segmentace směrovacích informací prostřednictvím standardní technologie Virtual Routing and Forwarding
SD-WAN fabric umožňuje aplikovat mikrosegmentaci provozu s využitím security group tags nebo ekvivalentní funkcionality
SD-WAN fabric umožňuje škálovat segmentaci infrastruktury minimálně na 60 VPN
SD-WAN fabric umožňuje v rámci VPN transportovat jak protokol IPv4, tak i protokol i IPv6
SD-WAN fabric umožňuje v rámci VPN transportovat IP multicast provoz s využitím protokolů PIM-ASM a PIM-SM
SD-WAN fabric umožňuje poskytovat aplikačnímu provozu různou kvalitu přenosové služby - QoS
SD-WAN fabric podporuje per tunnel QoS pro řízení provozu mezi centrální lokalitou a vzdálenými lokalitami
SD-WAN fabric podporuje Adaptive per-tunnel QoS umožňující adaptivní nastavení shaperu dle skutečně dostupného přenosového pásma na straně vzdálené (přijímající) lokality
SD-WAN fabric umožňuje aplikovat QoS policy per VPN/VRF
SD-WAN fabric umožňuje definovat různé topologie WAN sítě pro jednotlivé VPN sítě, např. Full-mesh, Hub-Spoke, Partial-mesh apod.
SD-WAN fabric podporuje per VPN funkce service-insertion a service-chaining umožňující automatické přesměrování vybraného aplikačního provozu na zařízení poskytující L4-L7 služby
SD-WAN fabric umožňuje řídit balancování datového provozu přes všechny dostupné transportní infrastruktury
SD-WAN fabric umožňuje směrovat aplikační provoz přes různé transportní infrastruktury (SD-WAN tunely) na základě následujících real-time SLA parametrů: • Zpoždění • Ztrátovost paketů • Jitter

Požadovaná funkcionalita/vlastnost
SD-WAN fabric umožňuje přiřazovat tzv. probe paketům, s jejichž pomocí měří SLA parametry jednotlivých SD-WAN tunelů, různé hodnoty DSCP
Pro pokročilé měření SLA metrik jednotlivých SD-WAN tunelů umožňuje SD-WAN fabric využívat časové známky (timestamps) nesené v záhlaví paketů transportovaných přes jednotlivé SD-WAN tunely
SD-WAN fabric umožňuje směrovat aplikační provoz přes různé transportní infrastruktury na základě real-time SLA metric jak pro unicast tak i pro multicast provoz
SD-WAN fabric umožňuje pro různé typy aplikačního provozu definovat preferovanou transportní infrastrukturu (SD-WAN tunel) včetně automatického failoveru na záložní transportní infrastrukturu
SD-WAN fabric umožňuje aplikovat síťové a aplikační politiky centralizovaně pro všechny lokality, regionálně pro vybrané lokality nebo lokálně pro každou lokalitu zvlášť
SD-WAN fabric umožňuje optimalizovat přístup koncových uživatelů v jednotlivých lokalitách WAN sítě k SaaS službám na základě real-time SLA parametrů jako je zpoždění a ztrátovost paketů
SD-WAN fabric pro měření real-time SLA parametrů SaaS služeb používá pokročilé mechanismy jako je např. HTTP ping
SD-WAN fabric umožňuje pro optimalizaci směrování provozu do M365 využívat telemetrická data poskytovaná M365 prostředím (M365 informed network routing)
SD-WAN fabric řešení je uvedeno mezi certifikovanými řešeními pro M365 informed network routing
SD-WAN fabric umožňuje optimalizaci směrování provozu do M365 dle M365 service-area
SD-WAN fabric umožňuje rozšířit WAN infrastrukturu včetně zajistění end-to-end síťových politik do public-cloud prostředí AWS, MS Azure a GCP
SD-WAN fabric umožňuje integraci s MS Azure vWAN prostředím
SD-WAN fabric umožňuje integraci s AWS Cloud WAN prostředím
SD-WAN fabric plně automatizuje implementaci konektivity ke službám IaaS, resp. SaaS prostřednictvím předdefinovaných workflows
SD-WAN fabric umožňuje realizovat per VPN lokální přístup do sítě Internet, tzv. Direct Internet Access včetně překladu IP adres prostřednictvím NAT44, NAT64 a NAT66
SD-WAN fabric umožňuje realizovat per VPN lokální přístup do sítě Internet, tzv. Direct Internet Access včetně stavové inspekce provozu prostřednictvím NG Firewall, který je integrální součástí pobočkového SD-WAN směrovače
SD-WAN fabric umožňuje realizovat per VPN lokální přístup do sítě Internet, tzv. Direct Internet Access včetně inspekce provozu prostřednictvím Intrusion Prevention System, který je integrální součástí pobočkového SD-WAN směrovače
SD-WAN fabric umožňuje realizovat per VPN lokální přístup do sítě Internet, tzv. Direct Internet Access včetně URL filtrace provozu na pobočkovém SD-WAN směrovači
SD-WAN fabric umožňuje realizovat per VPN lokální přístup do sítě Internet, tzv. Direct Internet Access včetně inspekce IPv4 i IPv6 provozu prostřednictvím funkce Advanced Malware Protection, která je integrální součástí pobočkového SD-WAN směrovače
SD-WAN fabric umožňuje realizovat per VPN lokální přístup do sítě Internet, tzv. Direct Internet Access včetně inspekce provozu prostřednictvím TLS 1.3 proxy, která je integrální součástí pobočkového SD-WAN směrovače

Požadovaná funkcionalita/vlastnost
SD-WAN fabric podporuje směrovací protokol OSPF včetně možnosti běžet instanci OSPF protokolu per VPN (VRF)
SD-WAN fabric podporuje směrovací protokol BGP včetně pokročilých funkcionalit jako je propagace AS-Path a eBGP multihop
SD-WAN fabric podporuje pokročilou detekci a klasifikaci jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)
SD-WAN fabric umožňuje v rámci DPI definovat signatury pro vlastní aplikace zákazníka
SD-WAN fabric umožňuje First Packet Matching pro skupinu aplikací M365
SD-WAN fabric zajišťuje kontinuální a granulární meření výkonnostních charakteristik jednotlivých aplikací a vlastní komunikační infrastruktury
SD-WAN fabric umožňuje monitorovat jednotlivé datové toky (všechny pakety) a exportovat monitorovaná data ve formátu IPFIX
SD-WAN fabric umožňuje monitorovat Application Response Time metriky pro jednotlivé datové toky
SD-WAN fabric umožňuje směrovat pouze vybraný aplikační provoz do cloud security infrastruktury
SD-WAN fabric zajišťuje vysokou dostupnost spojení s poskytovatelem cloud security služeb včetně možnosti load-balancovat provoz směrem k poskytovateli cloud security služeb
Management konzole pro správu SD-WAN fabric umožňuje Role Based Access Control
RBAC je možné aplikovat per lokalita/zařízení
RBAC je možné aplikovat pro konfiguraci zařízení i SD-WAN politiky
Management konzole pro správu SD-WAN fabric disponuje otevřeným API rozhraním pro integraci s externími systémy
SD-WAN Fabric poskytuje podrobnou visibilitu aplikačního provozu včetně měření výkonnosti jednotlivých přenášených aplikací a predikce potřebné šířky přenosového pásma pro zajištění kvalitního přenosu aplikačního provozu

Specifikace Centrálního automatizovaného managementu firewallů

Identifikace Centrálního automatizovaného managementu firwewallů:

Výrobce	**Palo Alto Networks**
Obchodní název	**Panorama Central Management**

Požadovaná funkcionalita/vlastnost
Zařízení typu centrální správa Firewallů ve formě virtuální appliance umístěné ve virtualizačním prostředí MSpWAN - On-Premis
Minimálně 250 centrálně spravovaných Firewallů včetně všech jejich funkcionalit a virtuálních kontextů a všech potřebných licencí pro centrální správu
Virtuální appliance pro správu firewallů nasazená v režimu vysoké dostupnosti (minimálně dvě appliance) ve dvou oddělených lokalitách

Požadovaná funkcionalita/vlastnost
Podpora režimu active-active i active-standby
Centrální správa musí podporovat sběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci
Centrální správa musí umožnit sběr minimálně 50 000 logových záznamů za vteřinu
Centrální správa musí umožnit minimálně 1 měsiční retenci záznamů při logování veškerého provozu ze všech spravovaných firewallů
Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní NGFW a zároveň přes grafické rozhraní centrálního managementu
Administrátor musí mít možnost importovat NGFW konfiguraci do centrálního managementu
Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat s grafickým rozhraním a způsobem konfigurace NGFW kvůli konzistenci a jednoduchosti přechodu mezi platformami
Administrátor musí mít možnost zapsat změny i při čekajících změnách od ostatních administrátorů
Centrální management musí umět v reálném čase zkontrolovat plánované změny v konfiguraci při zápisu a zablokovat ty, které neodpovídají předepsaným pravidlům
Centrální správa musí pro autentizaci a autorizaci administrátorů podporovat protokoly TACACS, LDAP, Radius, SAML a lokální databázi
Centrální správa musí podporovat vynucení multifaktorové autentizace
Centrální správa musí podporovat definování různých administrátorských rolí
Centrální správa musí podporovat vytváření šablon pro zjednodušení společné konfigurace na více firewallech
Centrální správa musí podporovat vytváření seskupování zařízení pro zjednodušení společné konfigurace na více firewallech a přiřazení jednotné politiky
Centrální správa musí podporovat hierarchické seskupování různých politik pro zjednodušení společné konfigurace na více firewallech (například: globální pravidla pro všechny firewally, plus pravidla dle lokality, plus lokální pravidla konkrétního firewallu)
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu
Pro reporty lze definovat template definující formát a obsah reportu
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, které umožňují editaci jako jsou CSV, HTML apod.
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí (např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.)
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu
Centrální správa firewallů musí umožňovat korelaci bezpečnostních událostí generovaných jednotlivými firewally (IPS, apod.), bez nutnosti instalace další HW nebo VM appliance

Požadovaná funkcionalita/vlastnost
Centrální správa musí podporovat integraci s autentizačními systémy pro možnost mapování uživatelských identit na IP adresy (získané uživatelské identity je možné použít pro vytváření bezpečnostních politik a monitoring událostí)
Centrální správa musí podporovat auditní logování konfiguračních změn
Centrální správa musí zobrazit rozdíl mezi stávající a novou konfigurací na jednotlivých firewallech (před instalací FW politiky)
Centrální správa musí umožňovat kopírování politik z jednoho FW (z jedné politiky) na jiný FW (do jiné politiky)
Centrální správa musí umožňovat konfiguraci pomocí objektů a jejich následnou úpravu
Centrální správa musí umožňovat vytvoření skupiny objektu a vkládání objektů do skupiny objektů, tyto objekty a skupiny objektů (síťové objekty, objekty portů…) musí být možné upravovat i přesto, že jsou nastavené v jakékoliv části konfigurace FW
Centrální správa umožňuje pravidelné zálohy konfigurace nebo částí konfigurace (FW pravidla, objekty, routing…) na externí úložiště pomocí protokolu SFTP nebo SCP nebo SMB
Centrální správa musí umožnit bezobslužnou implementaci nových firewallů s využitím zero trust provisioning (ZTP)

Specifikace Centrálního automatizovaného managementu Switchů

Identifikace Centrálního automatizovaného managementu Switchů:

Výrobce	**Cisco**
Obchodní název	**Cisco DNA Center Virtual Appliance**

Požadovaná funkcionalita/vlastnost
Zařízení typu centrální správa Switchů ve formě virtuální appliance umístěné ve virtualizačním prostředí MSpWAN - On-Premis
Minimálně 250 centrálně spravovaných Switchů včetně všech jejich funkcionalit a včetně potřebných licence pro centrální správu
Platforma nesmí být v cestě datovému toku sítě. To znamená, že veškerý datový provoz koncových bodů nebude muset procházet platformou pro jakoukoli komunikaci s jinými koncovými body / externí sítí
Platforma musí poskytovat webové rozhraní pro jednotnou správu drátové a bezdrátové sítě poskytující integrovaný pohled na drátovou i bezdrátovou síť. Poskytuje správci rychlý a snadný pohled na stav sítě, umožňující snadnou identifikaci výpadků, izolaci problémů v síti a obsahující doporučení pro identifikaci nápravy hlavních příčin
Platforma poskytuje grafické zobrazení topologie sítě s možností vyhledávání a exportu. Vytvoření mapy fyzické topologie sítě lokality na základě rolí jednotlivých síťových prvků softwarově definované sítě. Možnost umístění lokality do mapy na základě adresy lokality nebo GPS souřadnice. Možnost organizovat síťovou hierarchii organizace do oblastí, budov a pater
Automatizace poskytovaná platformou je založená na politikách. Zjednodušuje a abstrahuje od složitosti správy sítě při nasazování a vynucování politiky v celé síti

Požadovaná funkcionalita/vlastnost
Platforma umožňuje automatizaci nastavení standardních síťových služeb (DNS, DHCP, AAA, přístupová oprávnění, monitoring) pro síťová zařízení podle lokality
Platforma podporuje centralizovanou správu standardních konfigurací s využitím konfiguračních šablon
Platforma umožňuje automatizaci provozních změn – modifikaci chování síťového zařízení aplikací konfigurační šablony
Platforma musí umožnit kontrolu (náhled) plánované konfigurační změny před její aktivací na síťovém zařízení
Platforma musí poskytnout detailní informace o výsledku požadavku na provedení konfigurační změny
Platforma musí zobrazit informace o provedených konfiguračních změnách síťového zařízení včetně změn nerealizovaných centralizovaným síťovým kontrolérem – tzv. out-of-band změny
Platforma musí poskytovat podrobný soupis a inventář zařízení uspořádaný podle typu zařízení, jména, IP adresy, MAC adresy, firmware, sériového čísla a konfigurace. Tento inventář musí být možno automaticky aktualizovat minimálně po každých 30 minutách
Platforma musí poskytovat informace o stavu životního cyklu spravovaných síťových zařízení pro snadnou identifikaci zařízení se známým datem blížícího se konce podpory výrobce apod.
Platforma podporuje automatické zprovoznění nových zařízení – jejich nalezení, zajištění bezpečné komunikace s kontrolérem, zavedení do inventáře a pod správu, upgrade na požadovanou verzi programového vybavení a konfiguraci s využitím základní konfigurační šablony
Platforma podporuje tvorbu konfiguračních šablon v Apache Velocity Language a Jinja a jejich skládání do kompozitních šablon
Konfigurační šablony musí podporovat definici proměnných různých, definici jejich implicitních hodnot a vazbu na databázi platformy (např. seznam rozhraní konkrétního zařízení)
Aplikace šablon na zařízení musí být možná okamžitě nebo později v definovaném časovém okamžiku nebo pouze vygenerovat náhled konfigurace
Platforma musí poskytovat nástroj pro simulaci konfiguračních šablon
Šablony mohou být přiřazeny k zařízení na základě lokality, modelu a značky
Platforma umožňuje mít integrovaný modul síťové analýzy a také funkce kognitivní analýzy prostřednictvím Machine Learning pro řešení problémů se sítí
Přístup ke kontrolérům musí být možný na základě rolí (pouze čtení, povolené změny a administrátor)
Platforma musí poskytovat informace o provedených změnách (kdo, co, kdy) – auditní logy
Platforma musí podporovat následující standardní protokoly, které jí umožňují komunikovat se síťovými zařízeními: NETCONF, SSH, SNMP, HTTP(S)
Platforma musí podporovat autentizaci pomocí TACACS a RADIUS
Platforma musí poskytovat otevřená rozhraní API pro vytváření inteligentní, otevřené a programovatelné sítě/fabriky pro konfiguraci pokročilých automatizačních služeb
Platforma musí poskytovat otevřená rozhraní API pro zasílání událostí z monitoringu
Platforma musí podporovat rozhraní API REST (Representational State Transfer)
Platforma musí podporovat automatické aktualizování software kontroléru z cloudu přes cloud tethering
Platforma musí podporovat automatické aktualizace aplikací kontroléru prostřednictvím cloudového tetheringu

Požadovaná funkcionalita/vlastnost
Platforma musí podporovat režim redundance s plnou perzistencí dat pro vysokou dostupnost
Platforma musí umožňovat jednoduchou a centralizovanou definici síťových a bezpečnostních politik
Platforma musí podporovat integraci s dalšími bezpečnostními zařízeními prostřednictvím Platform Exchange GRID (pxGrid), který využívá mnoho dodavatelů zabezpečení, jako jsou Checkpoint, LogRhythm, Splunk, Huntsman, Infoblox, Ping Identity, Cisco ISE a mnoho dalších
Možnost registrace a správy příslušných licencí připojených síťových prvků
Kontrolér musí podporovat správu obrazů softwaru aktivních prvků, udržovat centrální úložiště obrazů programového vybavení zařízení a aplikovat je jednotlivě i najednou na více zařízení (například ve stohu)
Kontrolér musí podporovat správu obrazů softwarových oprav (patch) a aplikovat je jednotlivě i najednou na více zařízení (například ve stohu)
Kontrolér musí umožnit definovat softwarovou politiku, jaký konkrétní obraz softwaru aktivního prvku je v síti a / nebo v lokalitě standardem pro rodinu zařízení a / nebo roli zařízení (přístup, distribuce, jádro sítě)
Kontrolér musí umožnit operátorovi jednoduchou identifikaci aktivních prvků, které vyžadují změnu obrazu software z důvodu změny v softwarové politice nebo protože stávající obraz aktivního prvku není v souladu se platnou politikou
Funkce správy obrazu softwaru musí podporovat provádění předběžných kontrol inventáře zařízení ohledně dostupnosti doporučeného prostoru ve flash paměti. Po nasazení (aktualizaci softwarového obrazu) musí zkontrolovat úspěšnou aktivaci nainstalovaného obrazu
Platforma musí podporovat HTTPS, SFTP a SCP pro distribuci softwarových obrazů
Kontrolér musí podporovat plánování distribuce a aktivace obrazů softwaru na jednotlivá síťová zařízení. Distribuci a aktivaci musí být možno provést v rozdílný čas
Kontrolér musí být schopen indikovat, že softwarový obraz (verze programového vybavení) je zasažen bezpečnostní zranitelností
Kontrolér musí podporovat sladění charakteristik softwarového obrazu se softwarovou politikou u nově zprovozňovaných zařízení
Funkce kontroléru - Monitoring a analýza stavu sítě, řešení výpadků a potíží se sítí
Zobrazení informace o monitorované síti / vybrané části sítě
Zobrazení informace o monitorovaných aktivních prvcích
Zobrazení informace o připojených drátových koncových stanic a uživatelů
Zobrazení informace o využívaných aplikacích
Zobrazení informace o aplikacích používaných jednotlivými drátovými klienty
Detekce problémů se síťovými zařízeními
Uvedení doporučených nápravných kroků pro každý zjištěný výpadek nebo problém
Uchování minimálně 14 denní provozní historie sítě umožňující analýzu i řešení výpadků a problémů, ke kterým došlo v minulosti, stejnými postupy jako u právě probíhajících výpadků
Detailní zobrazení stavu a provozní historie síťového zařízení, souvisejících událostí, problémů a topologie připojení sousedních aktivních prvků v analyzovaném čase

Požadovaná funkcionalita/vlastnost
Detailní zobrazení stavu a provozní historie klienta, souvisejících událostí, problémů, detail síťového připojení v analyzovaném čase a přehled využívaných aplikací včetně výkonnostních parametrů (jitter, loss, latency, throughput)
Využití metod strojového učení (Machine Learning) lokálně
Využití metod automatického uvažování (Machine Reasoning) v rámci postupů pro řešení vybraných typů problémů
Automatické vytváření vzoru chování sítě pro identifikaci anomálií
Platforma poskytuje funkce pro automatizaci výměny vadného zařízení novým zařízením při zachování konfigurace a monitoring historie

3.3 Bezpečnostní dohled nad Infrastrukturou MSpWAN

Poskytovatel zřídí monitorovací a dohledové centrum jako dálkovou aplikační službu, které umožní Poskytovateli i Objednateli v reálném čase a nepřetržitě monitorovat stav Infrastruktury MSpWAN a poskytovaných Služeb Infrastruktury MSpWAN, stav dodržování parametrů SLA a veškeré významné výkonnostní a bezpečností parametry Infrastruktury MSpWAN a Služeb Infrastruktury MSpWAN („**Monitorovací centrum Infrastruktury MSpWAN**“).

Monitorovací centrum Infrastruktury MSpWAN bude integrováno do dohledových a monitorovacích nástrojů Objednatele přes standardizované integrační rozhraní.

Bezpečnostní dohled nad Infrastrukturou MSpWAN je realizován prostřednictvím

- Zařízení pro sběr dat
- Centrální vyšetřovací konzolí a
- Datovým uložištěm pro úchovu analyzovaných dat.

Specifikace zařízení pro sběr dat pro bezpečnostní analýzu

Identifikace zařízení pro sběr dat:

Výrobce	**Gigamon**
Obchodní název	**GigaVUE HC Packet Broker**
Model	**GigaVUE-HC1**
Part-number	**GFM-FM001** **GVS-HC101-HW** **GSS-HW-AHR-GMO** **GVS-HC100-SW-TM** **PCD-00003** **SMT-HC1-BN-CORE** **SMT-HC1-GEN2-DD1-SW-TM**

Požadovaná funkcionalita/vlastnost
Sběr síťových dat samostatně pro každou z lokalit DC Děkanka a DC Míčánky
Minimálně 2x 10 Gb/s rozhraní pro zpracování síťového provozu
Integrace se síťovým prostředím je zajištěna zrcadleným síťovým provozem, který je poskytování ze switchů pro DC
Možné rozšíření řešení o in-line způsobu zapojení pro metalické i optické komunikační trasy pomocí TAP
Možnost provádět filtrování síťového provozu před jeho předáním na výstupní rozhraní pro připojení analytických nástrojů. Cílem je umožnit předat jen potřebné typy komunikací pro každý připojený analytický nástroj.
Pravidla pro filtorvání provozu musejí být definovatelná podle 4. vrstvy ISO/OSI modelu.
Možnost provádět manipulace s provozem do monitorovacích zařízení: • Maskování citlivých informací – umožňuje bezpečnostním týmům skrýt citlivé informace a tím ochránit organizaci před porušováním nažízení plynoucích z ZoKB popř. GDPR. • Předávání jen vybrané části komunikací, které jsou předmětem zájmu připojeného monitorovacích zařízení - předávání jen hlaviček provozu bez obsahu paketů. • Doplňování dodatečných informací o zdroji monitorovaných dat pro lepší orientaci a obohacení monitoringu.
Monitorovaný provoz musí být v dodávaném řešení optimalizován: • Deduplikován • Odstranění nadbytečných údajů • Obohacen o metadata
Podpora visibility do šifrovaného provozu za předpokladu importu privátního klíče certifikátu.

Specifikace Centrální vyšetřovací konzole

Identifikace Centrální vyšetřovací konzole:

Výrobce	**Fidelis**
Obchodní název	**Fidelis Network**

Požadovaná funkcionalita/vlastnost
Detekce malwaru přenášeného přes jakýkoli nešifrovaný protokol.
Možnost importu detekčních pravidel s podporou formátů YARA a zdrojů specifikace TAXII/STYX.
Možnost importu úplného záznamu síťové komunikace ve formátu PCAP pro kontrolu, popis a hloubkovou analýzu.
Import popisu hrozeb od třetích stran a vlastních, které mohou být dodány ve formátech STIX, TAXII, CSV (podpora ThreatConnect).
Detekce zpětných volání malwaru Command & Control.

Požadovaná funkcionalita/vlastnost
Detekce pokusů o zneužití zranitelností na dálku prostřednictvím sítě.
Detekce malwaru zabaleného i hluboko v obsahu (v archivech a dalších složených dokumentech).
Identifikace spojení využívajících neočekávané nebo neznámé protokoly (např. nesoulad portů a protokolů).
Obsahová analýza pro detekci exfiltrace informací s možností nasazení v prostředí se značkami (klasifikátory) i bez nich (např. pomocí regulárních výrazů obsahových pravidel, vzorových šablon atp.).
Funkce obsahové analýzy detekuje informace přenášené i hluboko v obsahu, bez ohledu na hloubku vložení a bez ohledu na formát souboru.
Možnost definovat vlastní pravidla detekce nad libovolným typem přenášeného obsahu, charakteristikami chování nebo posloupností událostí v síti.
Systém bude schopen aplikovat aktualizované signatury na historický síťový provoz uložený v popisných metadatech po dobu požadované retence, aby našel nyní známý malware, který nebyl v minulosti detekován.
Detekce malwaru se provádí pomocí (všech níže specifikovaných způsobů): - signatur a pravidel, - heuristické analýzy, - vyhledávání typického chování (behaviorální analýza), - detekce anomálií.
Detekce anomálií pomocí modelů strojového učení a případné generování alarmů pro významné anomálie.
Pravidla analýzy provozu umožňují definovat podmínky vztahující se k přenášenému obsahu a parametrům aplikační vrstvy, například detekovat přenášené soubory, u nichž koncovky soborů neodpovídají obsahu nebo typická čísla portů neodpovídající typu detekovaného komunikačního protokolu.
Možnost definovat pravidla pro vyhledávání shody událostí nebo posloupnosti událostí v síťovém provozu a generovat výstrahy průběžnou analýzou okamžitých událostí a analýzou již uložených historických záznamů o provozu zpětně.
Systém musí klasifikovat události podle MITRE ATT&CK frameworku uvedením odpovídající techniky a/nebo taktiky útočníka. Vlastní pravidla lze definovat tak, aby také používala kategorie MITRE ATT&CK frameworku.
Retrospektivní analýza všech zaznamenaných údajů o chování sítě, která odhalí sled událostí vedoucích k projevům kybernetického incidentu.
Možnost definovat pravidla (komunikační matice) pro vyhodnocení oprávněnosti odchozí komunikace vůči definovaným kritickým informačním systémům pomocí kombinací parametrů: • IP adresa/seznam IP adres/rozsah adres, • Skutečný typ detekovaného protokolu (nezávisle na definovaném čísle portu TCP/UDP), • Čísla portů (TCP/UDP).
Vestavěná funkce pro vyšetřování, shromažďování stop a generování zprávy o incidentu.
Průběžné zaznamenávání informací o síťové komunikaci ve formě, která umožňuje pozdější analýzu (metadata).
Export úplného záznamu, předem popsaných síťových komunikací, ve formátu PCAP pro další zkoumání.
Pro následnou analýzu jsou k dispozici historické informace o provozu se stanovenou dobou uchování.
Systém podporuje efektivitu vyšetřování tím, že dokáže automatizovaně spojovat jednotlivé bezpečnostní události, které mají společnou příčinu, do jedné události (incidentu).
Extrakce obsahu souborů zachycených při jejich pohybu po síti pro forenzní účely pomocí systémové konzoly.

Požadovaná funkcionalita/vlastnost
Zaznamenané informace o provozu umožňují vyhledávat spojení podle libovolného atributu popisujícího spojení nebo pomocí logického výrazu s relačními operátory odkazujícími na atributy spojení.
Vestavěná podpora pro řízení životního cyklu tiketů pro distribuci úkolů mezi uživatele systému/vyšetřovatele.
Geolokace komunikujících stran.
Možnost vlastní definice geolokačních tabulek IP adres (pro geolokaci privátní IP segmentů).
V oblasti detekce a vyšetřování Advanced persistent threats (APT) musí systém splňovat požadavek na viditelnost stop daného útoku a dostupnost forenzních dat ze všech zachytitelných fází útoku APT (podle fází cyber-kill-chain).
Systém přiřazuje informace o uživatelském účtu k zaznamenanému síťovému spojení.
Schopnost automatizace pracovních postupů při nápravě kybernetických incidentů: • plně automatická reakce definovaná bezpečnostní politikou pro síťový provoz, • podporované metody: DROP při in-line zapojení, nebo TCP.
Reset pro out-of-band připojení.
Schopnost ukončit spojení na základě detekce.
Zdokumentované aplikační rozhraní pro integraci s dalšími bezpečnostními komponentami. Upřednostňujte rozhraní API http a XML nebo JSON.
Předpřipravené integrační vazby na aplikace typu SIEM.
Systém poskytuje webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní.
Dashboard a možnosti jeho úprav pro grafické zobrazení informací a podpory rozhodovacího procesu (alert triage).
Možnost detailního řízení přístupových práv pro více úrovní pracovníků SOC (analytici, operátoři, IT podpora, forenzní analytici, vyšetřovatelé).
Možnost napojení na ActiveDirectory/LDAP pro autentizaci uživatelů systému.
Jednotné uživatelské rozhraní pro veškerou analytiku, vyšetřování a reakci.
Systém je platforma pro forenzní analytiku, detekci, vyšetřování a řízení reakcí na zaznamenané kybernetické události.
Systém musí podporovat práci v hierarchickém režimu (včetně selektivní správy práv k informacím) pro případné budoucí zapojení podřízených organizací do bezpečnostního dohledu. Požadavek zahrnuje jednotné rozhraní pro vyšetřování, konfiguraci bezpečnostní politiky a správu řešení u všech podřízených organizací, vlastní rozhraní pro správu v každé podřízené organizaci a datová úložiště v každé podřízené organizaci.
Generování reportů dle předpřipravených šablon.
Tvorba a generování zákaznicky definovaných reportů.
Možnost nastavení automatického generování a odesílání reportů na emailové adresy.
Systém monitoruje svůj vnitřní chod a drží historické informace o událostech týkající se vlastního chodu a problémů.

Specifikace Datového uložiště pro úchovu analyzovaných dat

Identifikace Datového uložiště pro úchovu analyzovaných dat:

Výrobce	**Fidelis**
Obchodní název	**Fidelis Elevate**
Model	**Fidelis Network**
Part-number	**FNL-10G-30D-INT** **FNL-10G-30D-SUP-INT** **FNL-VM-CP+-SB-INT** **FNL-VM-CP+-SB-SUP-INT** **FNH-10G-INT** **FNH-CC10G-INT** **FNH-CXA4-INT**

Požadovaná funkcionalita/vlastnost
Analýza síťového provozu probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly a monitorovány jsou tedy všechny probíhající spojení na všech síťových portech monitorované infrastruktury.
Minimálně 10 Gb/s analyzovaných informací ze zařízení pro sběr síťových dat (průměr za 24 hodin)
Celková požadovaná retence všech historických dat o chování sítě v délce 30 dnů.
Metadata relevantní k detekovaným bezpečnostním událostem musí řešení uložit po dobu 12 měsíců.

3.4 Provoz Infrastruktury MSpWAN.

V rámci provozu Infrastruktury MSpWAN předpokládá Objednatel tyto základní oddělené datové toky:

1. **Uživatelský datový tok** – obsahuje provoz uživatelů směrem do Internetu nebo k aplikacím v datovém centru či v kraji či v resortu

2. **Serverový datový tok** – obsahuje provoz serveru či aplikace směrem do Internetu nebo k aplikacím v datovém centru či v kraji či v resortu

3. **Multimediální datový tok** – realizuje přenos dat při provozu videokonferenčních jednotek z organizačních složek Objednatele směrem do datových center Objednatele, kde je provozováno centrální řešení pro videokonferenční přenosy. Zároveň tento datový tok realizuje též přenos dat při IP telefonování mezi organizačními složkami Objednatele.

   Specifikace pro řízení datového toku videokonferenčního provozu:

   - Interaktivní video provoz by měl být v QoS označen jako DSCP AF41; nadměrný

provoz videokonferencí může být policerem QoS označen AF42 nebo AF43.

- Ztrátovost na lince by neměla být větší než 1%.
- Jednosměrná latence by neměla být větší než 150 ms.
- Jitter by neměl být větší než 30 ms.

Specifikace pro řízení datového toku pro IP telefonii:

- Provoz by měl být QoS označen jako DSCP EF podle základní QoS a RFC 3246.
- Ztrátovost na lince by neměla být větší než 1%.
- Jednosměrná latence (mouth to ear) by neměla být delší než 150 ms.
- Průměrný jednosměrný jitter by měl být zacílen na méně než 30 ms.

Objednatel upozorňuje, že v budoucnu může vzniknout potřeba definování dalších datových toků a Poskytovatel je povinen zajistit přiměřenou součinnost při jejich specifikaci a vytváření.

V rámci provozu Infrastruktury MSpWAN požaduje Objednatel po Poskytovateli níže uvedené činnosti a aktivity:

Fyzické úkony

- Fyzická instalace HW zařízení a jeho zapojení do sítě včetně fyzického kabelového patchování (propojování kabeláží)
- Instalace Software appliance a jeho zaintegrování do sítě a nastavení
- Kompletní HW on-site podporu v případě chybového stavu, kde to bude povaha chybového stavu vyžadovat (režim 24x7)
- Podpora výměny a opravy HW zařízení (režim 24x7)
- Realizace Servisních Požadavků
- Realizace Změnových Požadavků

Konfigurační úkony

- Administrace HW či SW prostředí, včetně zálohy konfigurací a inventarizace
- Administrace a konfigurace síťových a bezpečnostních zařízení
- Logická správa celé Infrastruktury MSpWAN na centrální úrovni (včetně výpočetního prostředí a centrálních administrátorských nástrojů) i na lokální úrovni jednotlivých složek (kompletní provozní správa dle parametrů SLA včetně zajištění vazeb na ostatní infrastrukturní celky)
- Konfigurace a optimalizace WAN spojení, monitorování dostupnosti a výkonu

- Definice směrovacích politik
- Definice analyzovaného obsahu, detekčních pravidel, výjimek z analytiky
- Zajištění konfigurace filtrování zrcadleného provozu určeného k analýze
- Optimalizace detekčních pravidel ve spolupráci se správci klíčových systémů
- Dešifrování specifického provozu pro hloubkovou analýzu
- Monitoring kvality vyhodnocovaných dat
- Identifikace anomálií v analyzovaných datech
- Konfigurace a implementace bezpečnostních politik pro MSpWAN
- Zajištění propojení jednotlivých lokalit s datovými centry dle definovaných šířek pásma pro jednotlivé lokality
- Konfigurace a optimalizace WAN spojení, monitorování dostupnosti a výkonu
- Správa přístupových práv, sledování síťového provozu a reakce na bezpečnostní incidenty
- Optimalizace distribuce přístupových bodů, sledování výkonu MSpWAN prostředí
- Monitorování a optimalizace šířky pásma pro zajištění dostatečné rychlosti přenosu dat
- Konfigurace šifrování, monitorování připojení a implementace bezpečnostních politik pro MSpWAN
- Pravidelná aktualizace firmware, monitorování vytížení a provádění diagnostiky
- Testování systémových záplat, aktualizací a nových funkcionalit před jejich implementací
- Aktualizace síťových prvků, sledování bezpečnostních incidentů a auditování bezpečnostních politik
- Aktualizace centrálních automatizačních managementů, sledování bezpečnostních incidentů a auditování bezpečnostních politik
- Realizace Servisních Požadavků
- Realizace Změnových Požadavků

Supportní úkony

- Vzdálený monitoring instalovaných HW a SW zařízení/appliancí a síťových zařízení
- Proaktivní monitoring chybových stavů a detekci vadných komponent včetně jejich odstraňování
- Monitorování výpadků a rychlá reakce na ně pro minimalizaci přerušení provozu Infrastruktury MSpWAN

- Sledování latence pro zajištění rychlé a efektivní komunikace
- Zajištění komunikace s výrobcem pro instalovaná zařízení (např. při otevírání ticketu s výrobcem a jeho následné řešení)
- Podpora při komunikaci a zakládaní servisních požadavků na třetí strany dle poskytnutých servisních smluv – typicky se jedná o komunikaci s operátory poskytující konektivitu v rámci KIVS
- Dokumentaci průběhu řešení problémů, poruchových stavů a provozních požadavků prostřednictvím ServiceDesk systému v souladu s Přílohou č. 2 této Smlouvy.
- Realizace Servisních Požadavků
- Realizace Změnových Požadavků

Architektonický dohled

- Návrhy designu architektury dle nároků aplikačních služeb či obecných trendů – Objednatel očekává proaktivní návrhy designu/redesignu a optimalizace či návrhy změn platforem HW/SW (pouze informativního charakteru).
- V případě menšího dopadu doporučené změny se bude realizovat v rámci zrychleného schvalování s daným útvarem, kterého se změna týká.
- V případě většího dopadu doporučené změny se bude změna projednávat s kompetentními útvary Objednatele (odpovědnými za provoz i bezpečnost).
- Návrhy optimalizace aplikačních a síťových komponent pro zajištění transparentnosti analyzovaných dat, a zároveň dosažení tzv. best practice v oblasti IT a SW architektury. Doporučení na minimalizace tzv. false positive optimalizací pracovních postupů administrátorů a uživatelů.
- Konzultace pro zvýšení efektivity bezpečnostní analýzy.
- Konzultace a podporu při implementaci nových služeb
- Konzultace a posouzení Servisních Požadavků
- Konzultace a posouzení Změnových Požadavků

Administrativní, dokumentační a podpůrné úkony

- Konfigurace Infrastruktury MSpWAN
- Správa detekčních scénářů včetně pravidelné optimalizace.
- Provádění pravidelné remote profylaxe SW/HW (remote kontrola healtcheck HW např. zdroje, větráky, CPU, RAM, HDD dále SW např. logy, systémové hlášení, errorové stavy) - profylaxe by měla zahrnovat takovou kontrolu zařízení/software, která na zařízení případně identifikuje chybový stav či odhalí možné chybové chování dříve, než se projeví jeho dopad. Profylaxe bude probíhat 1x za půl roku a bude vystaven summary

report, který zahrnuje zhodnocení stavu zařízení, případné chyby/errory/nestandardní parametry a budou stanoveny/předloženy nápravná opatření Zadavateli pro zhodnocení

- Udržování provozní dokumentace (aktuální konfigurace zařízení, logické a fyzické zapojení, servisní účty, konfigurační změny v souvislosti se změnovými požadavky a inventarizace použitého programového vybavení) a potřebných provozních manuálů
- Běžné reporty prováděných prací na měsíční bázi a Ad hoc/pravidelné automatizované reporty generovatelné prostřednictvím aplikačních rozhraní daného zařízení

Pokud není uvedeno jinak, budou výše uvedené úkony provozu Infrastruktury MSpWAN prováděné v režimu 8x5 v pracovních dnech[1] od 8:00 do 16:00.

Za účelem zajištění provozu Infrastruktury MSpWAN je Poskytovatel povinen průběžně provádět:

- **Monitorování výkonu:**

  Aktivita Poskytovatele: Monitorování výkonnostních metrik MSpWAN sítě a služeb v reálném čase nebo téměř v reálném čase.

  Cíl aktivity: Zajistit optimální úroveň výkonu, identifikovat úzká místa nebo zpomalení a podniknout preventivní opatření k udržení standardů výkonu.

- **Monitorování dostupnosti:**

  Aktivita Poskytovatele: Nepřetržité kontrolování dostupnosti IT zdrojů, jako jsou routery, firewally, switche, servery, aplikace (orchestratory).

  Cíl aktivity: Zajistit vysokou dostupnost detekcí a řešením výpadků nebo přerušení co nejdříve, minimalizovat dopad na Organizační složky.

- **Bezpečnostní monitoring:**

  Aktivita Poskytovatele: Monitorování bezpečnostních událostí, anomálií a potenciálních hrozeb v Infrastruktuře MSpWAN.

  Cíl aktivity: Detekce pokusů o neoprávněný přístup, infekcí malwaru, porušení dat nebo jiných bezpečnostních incidentů včas k minimalizaci rizik a ochraně citlivých informací.

- **Detekce a odpověď na incidenty:**

  Aktivita Poskytovatele: Monitorování systémů k detekci a rychlé odpovědi na

[1] Pracovním dnem je míněn kterýkoli den, kromě soboty a neděle a dnů, na něž připadá státní svátek nebo jiný svátek podle platných a účinných právních předpisů České republiky.

incidenty.

Cíl aktivity: Minimalizace dopadu incidentů identifikací problémů včas, vyvolání výstrah a zahájení procesů řízení incidentů pro rychlé obnovení služeb.

- **Plánování kapacity:**

  Aktivita Poskytovatele: Monitorování trendů využití zdrojů (CPU, paměť, úložiště, šířka pásma sítě) pro předpověď budoucích potřeb kapacity.

  Cíl aktivity: Zajistit dostatečnou kapacitu pro efektivní zpracování současných a předpokládaných zátěží, vyhnutí se degradaci výkonu nebo přerušení služeb kvůli omezením zdrojů.

- **Výstrahy a notifikace:**

  Aktivita Poskytovatele: Nastavení výstrah na základě předem definovaných trigerů nebo abnormálních vzorců ve sledovaných metrikách.

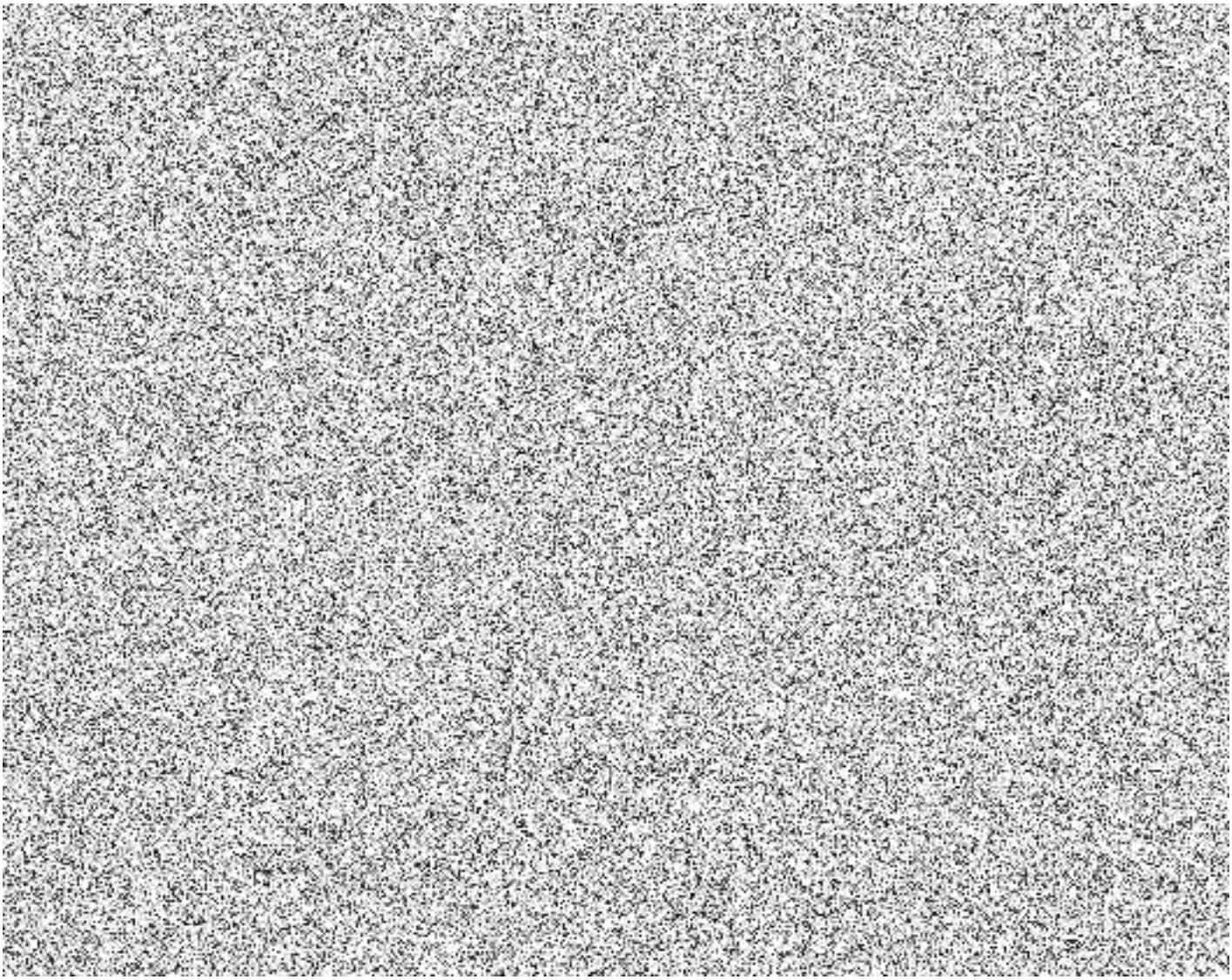
  Cíl aktivity: Okamžitě informovat IT týmy nebo zainteresované strany o kritických problémech, umožňující včasný zásah a řešení.

- **Zaznamenávání a reporting:**

  Aktivita Poskytovatele: Zaznamenávání všech relevantních informací o monitorovaných událostech a příprava reporting zpráv.

  Cíl aktivity: Poskytnutí strukturovaných reportů a analýz pro podporu strategických rozhodnutí a zlepšení IT prostředí.

Příloha č. 1A – Hlavní komunikační centrum



Hlavní komunikační centrum je tvořeno:

- 2 kusy routerů zapojenými redundantně dle obrázku výše.

Předpokládaná rychlost připojení k Infrastruktuře MSpWAN nepřekročí 100Gp/s.

1 Identifikace routerů

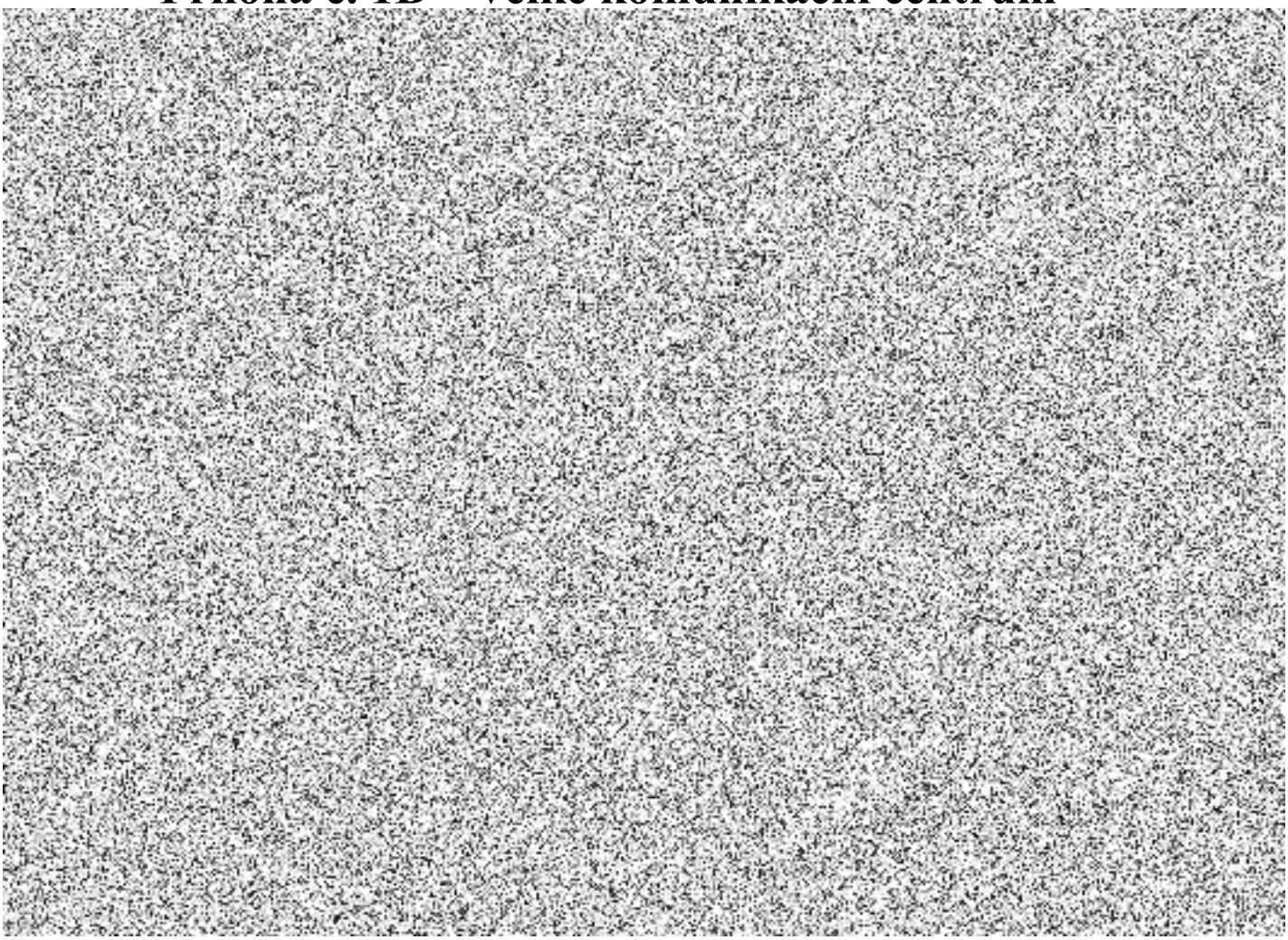
Výrobce	**Cisco**
Obchodní název	**Cisco Catalyst 8500-20X6C Edge Platform**
Model	**C8500-20X6C**
Part-number	**C8500-20X6C**

Požadované funkcionality a vlastnosti

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Typ zařízení: Směrovač	
Fixní formát zařízení	
Minimálně 20 portů 1/10 GigabitEthernet s volitelným fyzickým rozhraním typu SFP+	20
Minimálně 6 portů 40/100 GigabitEthernet s volitelným fyzickým rozhraním typu QSFP+	6
Interní redundantní AC napájecí zdroj 230V vyměnitelný za provozu	
Propustnost systému minimálně 500 Gb/s	500 Gb/s
Podpora jumbo frames, min. 9200 bytes	
OSPFv2, OSPFv3	
BGPv4, MP-BGP	
First Hop Redundancy Protokol (VRRP nebo HSRP)	
Interface tracker pro FHRP	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM ASM)	
IGMPv2, IGMPv3	
DHCP server pro IPv4	
DHCP relay pro IPv4	
Makrosegmentace provozu s využitím Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	
VRF aware směrovací protokoly, min. OSPF a BGP	
Minimálně 64 oddělených (nezávislých) směrovacích tabulek	64
Mikrosegmentace provozu s využitím security group tags nebo ekvivalentní funkcionality	
Možnost aplikovat ACL pro jednotlivé security group tags	
QoS classification – ACL, DSCP based	
QoS marking	
QoS Shaping and Policing	
Priority queuing	
Hierarchical QoS	
IPSec AES-GCM-256	
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	
Agregovaný šifrovací výkon pro IPSec AES-GCM-256 (IMIX provoz) minimálně 100Gb/s	100 Gb/s
IPSec IKEv2	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
IEEE 802.1AE (GCM-AES-256) na všech 1/10/40/100GE portech
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) včetně možnosti definovat signatury pro vlastní aplikace
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení
SSHv2
CLI rozhraní
Programovatelnost prostřednictvím NETCONF/YANG
SNMPv2/v3
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
NTPv3 server
Možnost plně integrovat směrovač do SD-WAN infrastruktury, jejíž funkční specifikace je uvedena ve specifikaci Katalogového listu SL03 - Služba Provoz centrálního automatizovaného managementu MSpWAN v oblasti Centrálného automatizovaného managementu Routerů MSpWAN

Příloha č. 1B – Velké komunikační centrum



Zapojení prvků Velkého komunikačního centra je redundantní a je na obrázku výše.

Předpokládaná rychlost připojení k Infrastruktuře MSpWAN nepřekročí 10Gp/s.

1 Identifikace routerů

Výrobce	**Cisco**
Obchodní název	**Cisco Catalyst 8500 Series 4x SFP+ and 8x SFP, 4x10GE, 8x1GE**
Model	**C8500L-8S4X**
Part-number	**C8500L-8S4X**

Požadované funkcionality a vlastnosti routerů

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Typ zařízení: Směrovač

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Fixní formát zařízení	
Minimálně 8 portů GigabitEthernet s volitelným fyzickým rozhraním typu SFP	8
Minimálně 4 porty 1/10 GigabitEthernet s volitelným fyzickým rozhraním typu SFP+	4
Interní redundantní AC napájecí zdroj 230V vyměnitelný za provozu	
Propustnost systému minimálně 35GB/s	39 Gb/s
Podpora jumbo frames, min. 9200 bytes	
OSPFv2, OSPFv3	
BGPv4, MP-BGP	
First Hop Redundancy Protokol (VRRP nebo HSRP)	
Interface tracker pro FHRP	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM ASM)	
IGMPv2, IGMPv3	
DHCP server pro IPv4	
DHCP relay pro IPv4	
Makrosegmentace provozu s využitím Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	
VRF aware směrovací protokoly, min. OSPF a BGP	
Minimálně 64 oddělených (nezávislých) směrovacích tabulek	64
Mikrosegmentace provozu s využitím security group tags nebo ekvivalentní funkcionality	
Možnost aplikovat ACL pro jednotlivé security group tags	
QoS classification – ACL, DSCP based	
QoS marking	
QoS Shaping and Policing	
Priority queuing	
Hierarchical QoS	
Application aware Zone-based firewall	
IPS/IDS	
URL Filtering	
Advanced Malware Protection	
TLS 1.3 proxy	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
IPSec AES-GCM-256	
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	
Agregovaný šifrovací výkon pro IPSec AES-GCM-256 (IMIX provoz) minimálně 10Gb/s	10 Gb/s
IPSec IKEv2	
IEEE 802.1AE (GCM-AES-256) na všech 1/10GE portech	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) včetně možnosti definovat signatury pro vlastní aplikace	
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	
SSHv2	
CLI rozhraní	
Programovatelnost prostřednictvím NETCONF/YANG	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	
Možnost plně integrovat směrovač do SD-WAN infrastruktury, jejíž funkční specifikace je uvedena ve specifikaci Katalogového listu SL03 - Služba Provoz centrálního automatizovaného managementu MSpWAN v oblasti Centrálného automatizovaného managementu Routerů MSpWAN	

2 Identifikace firewallů

Výrobce	**Palo Alto Networks**
Obchodní název	**Palo Alto Networks PA-3420**
Model	**PA-3420**
Part-number	**PAN-PA-3420**

Požadované funkcionality a vlastnosti firewallů

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Zařízení typu next generation firewall ve formě fyzické HW appliance	
Součástí dodávky je firewall, jeho licenční pokrytí a podpora/maintenance výrobce nabízeného řešení.	
Režim podpory výrobce nabízeného řešení je vyžadován minimálně v rozsahu 24/7, NBD	
Řešení se umístilo v posledních 6 letech (2018-2023) alespoň jednou v kvadrantu "leaders" v hodnocení Gartner Magic Quadrant for Network Firewalls	
Uchazeč uvede název výrobce řešení a specifikace nabízeného modelu, včetně výpisu všech konkrétních modulů a licencí, které jsou součástí nabídky	
Nabízené řešení je jako celek tvořeno komponenty jednoho výrobce, včetně používaných signatur, databází a zastřešeno jednotnou podporou výrobce.	
Je požadováno HA řešení složené minimálně ze dvou firewallů zapojených v active-passive nebo active-active zapojení	
Veškeré výkonové parametry musí HA řešení plnit i při výpadku či plánované odstávce jednoho z firewallů.	
Modul pro zpracování dat musí být v architektuře firewallu oddělen alespoň na úrovni CPU jader od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému negativnímu ovlivnění. Pokud je konfigurace odděleného managementu konfigurovatelná a má dopad na výkonové parametry, je nutno toto zohlednit pro splnění požadavků na propustnost	
Zadavatel vzhledem k požadované maximální úrovni zabezpečení síťového provozu vyžaduje kompletní inspekci veškerého síťového provozu s využitím komplexních detekcí na úrovni IPS, AV, DNS, URL, zero day útoků. Využívá-li nabízená technologie optimalizaci výkonostních parametrů s využitím funkcí mají negativní či kompromisní dopad na uroveň bezpečnostní kontroly síťového provozu, nelze je při plnění výkonostních parametrů uvažovat. Jedná se například o kontrolu pouze vybraných částí/vzorků provozu.	
Všechny výkonostní parametry musí být uvedeny v real world mix paketech, tzv. "application mix"	
Firewall musí obsahovat minimálně RJ45 dedikovaný port pro správu o rychlosti 1Gb/s	1Gb/s RJ45 OOBM, RJ-45 consolový port, USB
Propustnost FW při plné aplikační kontrole pro IMIX provoz a zapnutí všech dostupných signatur a kontrol IPS a AV, URL, DNS, IoT, SSH inspekci, sandboxingu a zapnutém logování minimálně 10 Gb/s (app mix)	10 Gb/s
Počet současných spojení minimálně 2 000 000	2 200 000
Počet nových spojení za sekundu minimálně 200 000	220 000
Zařízení je rozměrově kompatibilní s 19" rozvaděčem, maximální výška 1U	
Firewall obsahuje datové porty rychlosti minimálně: 10 portů 1Gbps (fyzické metalické) 10 portů datové porty rychlosti 10Gbps (SFP+) 4 porty datové porty rychlosti 25Gbps (SFP28)	 12x 1Gb/s 10x 1/10Gb/s SFP+ 4x 25Gb/s SFP28
Firewall obsahuje minimálně 1 dedikovaný port pro HA propojení firewallů (SFP+) rychlostí 10 Gb/s	2x 1Gb/s RJ45 1x 10Gb/s SFP+

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat virtuální kontexty
Součástí dodávky je příslušenství pro montáž do racku ve formě ližin či pevného ukotvení
Firewall musí obsahovat redundantní napájecí zdroj
Firewall musí plně podporovat IPv4 i IPv6
Firewall musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP
Firewall musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64
Firewall musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)
Firewall musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)
Firewall musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směrování.
Firewall musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směrování
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel
Firewall musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let
Firewall musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury sítě
Firewall musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů
Firewall musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty
Firewall musí obsahovat předdefinované threshholdy pro známé aplikační kategorie
Firewall musí mít schopnost provádět FEC (Forward Error Correction)
Firewall musí mít schopnost provádět per-application split tunneling
Firewall musí podporovat kompletní správu z centrálního prvku
Firewall musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu všech síťových a bezpečnostních funkcí v případě výpadku centrálního management prvku
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management prvku
Připojení ke GUI musí podporovat šifrování TLSv1.3
GUI musí obsahovat offline kontextovou nápovědu.
Firewall musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování
Firewall musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování
Firewall musí umožňovat automatickou konfiguraci použitím konfiguračních šablon na připojeném USB flash disku
Firewall musí podporovat možnost dodání předkonfigurovaného zařízení výrobcem pro bezobslužnou konfiguraci pomocí ZTP.
Firewall musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát
Firewall musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat nativní nástroj pro odchycení provozu
Firewall musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)
Firewall management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí vlastního firewallu
Firewall s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz
Firewall musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla
Definovaná aplikace musí představovat "match kritérium" při policy lookup
Firewall musí podporovat identifikaci aplikací napříč všemi porty/protokoly
Firewall musí podporovat identifikaci aplikací na nestandardních portech
Identifikace aplikace musí probíhat přímo ve firewallu
Firewall musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping
Firewall musí podporovat řízení neznámého provozu
Firewall musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla
Uživatelská identita musí představovat "match kritérium" při policy lookup
Firewall musí umožňovat automatický přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček
Firewall musí podporovat kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná
Firewall podporuje dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům
Firewall podporuje dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru
Dešifrovaný provoz lze definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita
Firewall podporuje OCSP (Online Certificate Status Protocol) pro kontrolu platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy
Firewall podporuje dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
Firewall musí poskytovat možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)
Firewall musí podporovat prioritizaci provozu na základě DSCP
Firewall musí podporovat prioritizaci provozu na základě Identifikované aplikace
Firewall musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita
Firewall musí obsahovat lokální úložiště logů
Firewall musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI
Firewall musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL
Firewall musí podporovat přeposílání logů na zařízení třetích stran
Firewall musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla
Firewall musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní Firewall
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB
Sandbox systém musí být od stejného výrobce jako je firewall, ale nemusí být HW součástí NGFW
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro firewall, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní firewallu
Aktualizace zero-day signatur musí být instalována do firewallu v reálnem čase, čili s nulovou prodlevou
Firewall musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod
Firewall musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu
Firewall musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky
Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí
Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita
Sandbox musí rozpoznat, které závislosti malware potřebuje k tomu, aby se spustil a umí je nasimulovat
Firewall musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu
Firewall musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve Firewall. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla
Firewall musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve firewallu. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB
Firewall musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci
Firewall musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů. Firewall musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů
Firewall musí podporovat import SNORT signatur
Firewall musí pro přístup ke kritickým aplikacím poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci. Tato vlastnost musí být konfigurovatelná na úrovní bezpečnostního pravidla
Firewall musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí poskytovat funkci k ochraně proti tzv. drive-by downloadům. Způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru
Firewall musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vratí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane
Firewall musí umět zabránit neznámým injekčním útokům jako je SQL a Command Injection útoky pomocí strojového učení
Firewall musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase
Firewall musí umět rozpoznat komunikaci ukrytou v DoH (DNS-over-HTTPS) požadavcích a aplikovat potřebná DNS bezpečnostní pravidla v reálném čase
Firewall musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.
Firewall musí umožnit detekci a kategorizaci zcizených či napadených domén a zneužití DNS v reálném čase pomocí strojového učení přímo na firewallu nebo pomocí cloudové služby
Podpora post-kvantového šifrování minimálně v rámci IKEv2 a IPsec. Firewall musí podporovat výměnu a vytváření hybridních klíčů založených na RFC 9242 a RFC 9370.
Firewall musí obsahovat nativní podporu pro využívání databáze URL
URL databáze musí být od stejného výrobce jako je firewall
Firewall musí být schopen použít URL kategorii v definici bezpečnostního pravidla
Firewall musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL
Firewall musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní firewallu bez nutnosti kontaktování technické podpory

3 Identifikace switchů

Výrobce	**Cisco**
Obchodní název	**Catalyst 9300 24-port data only, Network Advantage**
Model	**C9300-24T-A**
Part-number	**C9300-24T-A**

Požadované funkcionality a vlastnosti switchů

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
L2/L3 přepínače
Stohovatelný formát přepínače

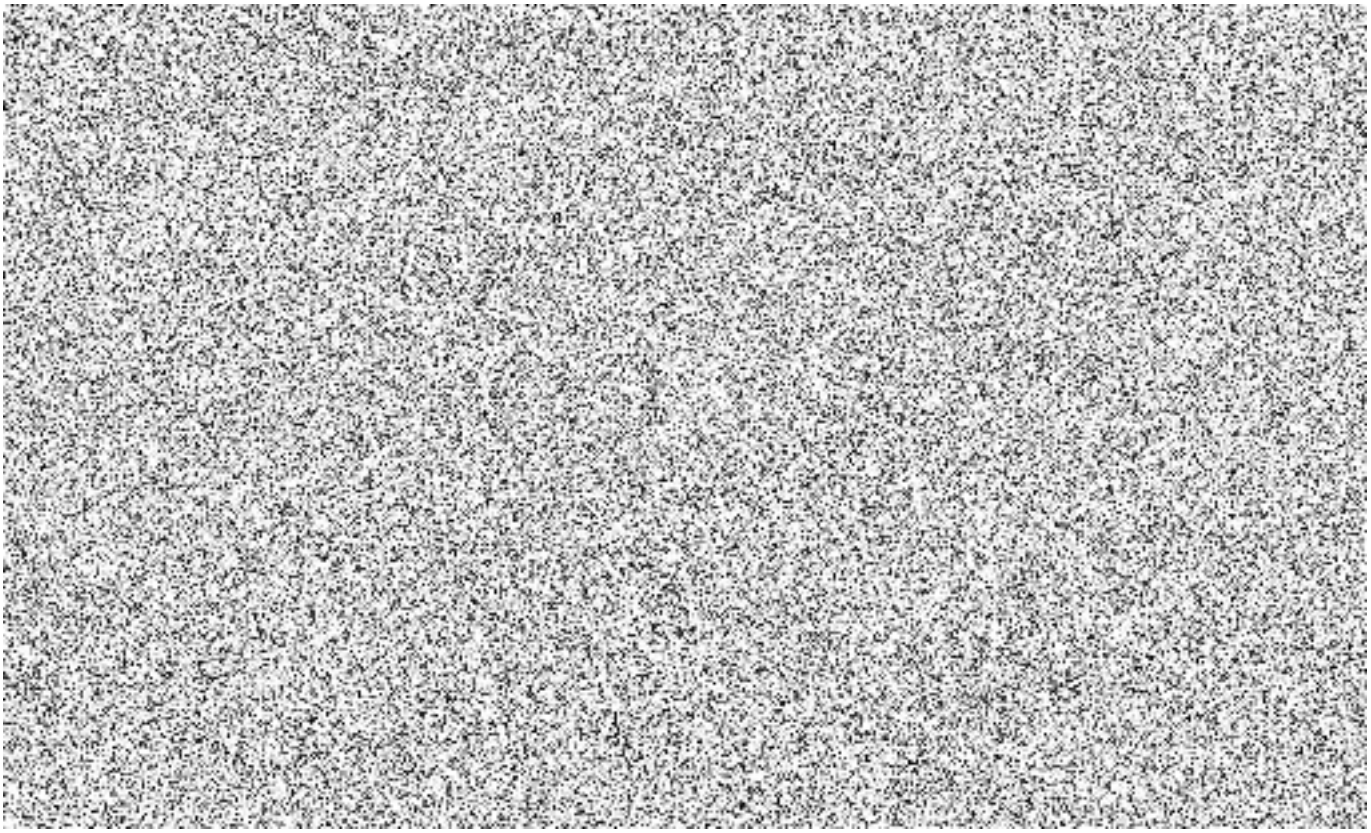
Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Minimálně 2 dedikované stohovací porty	2
Možnost stohování minimální 8 zařízení ve stohu	8
Kapacita sběrnice stohu minimálně 480 Gb/s	480
Stateful Switch Over v rámci stohu	
Přepínací kapacita minimálně 208 Gb/s	208 Gb/s
Paketový výkon přepínače minimálně 150 Mb/s	154 Mpps
Formát zařízení 1RU	
Velikost sdíleného systémového bufferu minimálně 16 MB	16 MB
Redundantní ventilátory vyměnitelné za chodu zařízení	
Možnost instalovat interní redundantní napájecí zdroj	
Možnost redundance zdrojů v režimu N+1	
Stohovací zdrojový kabel vyžadován	
Možnost stohování přes dedikované porty, bez snížení počtu použitelných ethernetových portů	
Stateful Switch Over v rámci stohu	
Minimálně 24 portů 10/100/1000Mbps Base-TX	24
Možnost přepínač rožšířit o modul s volitelným fyzickým rozhraním	
Rozšiřující modul s volitelným fyzickým rozhraním	
Rozšiřující modul s 8x1/10Gbps porty s volitelným fyzickým rozhraním typu SFP+	
Velikost MAC address tabulky minimálně 32 0000 MAC adress	32 000
Minimálně 32 000 IPv4 routes	32 000
Minimálně 16 000 IPv6 routes	16 000
Minimálně 5 120 konfigurovatelných security ACL	5 120
IEEE 802.3ad (Link Aggregation)	
IEEE 802.3ad přes více přepínačů ve stohu -bo více šasis	
Minimálně 8 li-k jako součást Link Aggregation Group trunku	
Minimální 128 konfigurovatelných Link Aggregation Group trunků	128
IEEE 802.1Q	
Minimální 1 000 aktivních VLAN	1024
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	
RADIUS CoA	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Podpora instance spanning-tree protokolu per VLAN	
IEEE 802.1w - Rapid Spanning Tree Protocol	
Protokol MVRP -bo VTP pro definici a správu VLAN sítí	
Podpora Jumbo rámců (minimálně 9 198 bytes)	9198
Detekce protilehlého zařízení (např. CDP -bo LLDP)	
Směrování protokolů IPv4 a IPv6 v hardware	
OSPFv2	
OSPFv3	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	
ISIS	
BGPv4	
VXLAN s BGP EVPN	
Policy based routing uvnitř VRF	
Graceful Insertion and Removal	
IP Multicast (PIM SSM, PIM SM)	
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	
MPLS VPN	
MPLS VPN přes GRE tunely	
MPLS VPN - 6VPE	
First Hop Redundancy Protokol (např. VRRP, HSRP)	
Reverse path check (uRPF) pro IPv4 i IPv6	
IGMPv2, IGMPv3	
IGMP snooping	
MLD snooping	
DHCP relay	
Minimální 8 HW QoS front	8
QoS classification – ACL, DSCP, CoS based	
QoS marking - DSCP, CoS	
QoS - Strict Priority Queue	
Automatické nastavení QoS parametrů (AutoQoS -bo ekvivalentní)	
QoS Policing	
QoS-Per Flow policing	
QoS-minimálně 2 úrovně Hierarchical QoS	2

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
First Hop Redundancy Protokol pro IPv6 (HSRP -bo VRRP)
IPv6 services (Tel-t, SSH, Syslog, DHCP)
IPv6 QoS
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)
IPv6 Port ACL, VLAN ACL
Možnost definovat povolené MAC adresy na portu
PACL, VACL
IEEE 802.1ae (AES-GCM-128) na uplink portech
IEEE 802.1ae (AES-GCM-256) na uplink portech
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy
Bezpečnostní funkce umožňující ochranu proti připojení -autorizovaného DHCP serveru
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů
Podpora SUDI (IEEE 802.1AR) autentizace
IEEE 802.3az
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
Multicast DNS (mDNS) gateway
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX
Full Flexible Netflow
SSHv2
CLI rozhraní
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Python scripting
Linux shell
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení
Application hosting
Aplikace softwarových záplat, nikoli povyšování celého firmware
Streaming telemetrie prostřednictvím NETCONF/XML
SNMPv2/v3
Podpora -twork boot (iPXE) pres IPv4 i IPv6
Inventarizovatelnost komponent integrovanou RFID identifikací
TACACS+ -bo RADIUS klient pro AAA (autentizace, autorizace, accounting)
AVC (NBAR2)
Vzdálený port mirroring (ERSPAN)
NTPv3 server

Příloha č. 1C – Střední komunikační centrum



Prvky Středního komunikačního centra jsou zapojené neredundantně dle obrázku výše.

Předpokládaná rychlost připojení k Infrastruktuře MSpWAN nepřekročí 5Gp/s.

1 Identifikace routeru

Výrobce	**Cisco**
Obchodní název	**Cisco Catalyst C8300-1N1S-4T2X Router**
Model	**C8300-1N1S-4T2X**
Part-number	**C8300-1N1S-4T2X**

Požadované funkcionality a vlastnosti routeru

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Typ zařízení: Směrovač	
Modulární formát zařízení	
Minimálně 4x 10/100/1000Base-T porty GigabitEthernet	4
Minimálně 2 porty 1/10 GigabitEthernet s volitelným fyzickým rozhraním typu SFP+	2
Interní redundantní AC napájecí zdroj 230V vyměnitelný za provozu	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Minimálně 3 volné sloty pro rozšiřující komunikační moduly	Ano
Možnost rozšířit směrovač o Wireless WAN modul s rozhraním 5G/LTE s následujícími parametry: 5G (Sub 6GHz) LTE category 20 Podpora dual SIM	
Propustnost systému minimálně 19 Gb/s	19 Gb/s
Podpora jumbo frames o velikosti minimálně 9 200 bytes	Ano
OSPFv2, OSPFv3	
BGPv4, MP-BGP	
First Hop Redundancy Protokol (VRRP nebo HSRP)	
Interface tracker pro FHRP	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM ASM)	
IGMPv2, IGMPv3	
DHCP server pro IPv4	
DHCP relay pro IPv4	
Makrosegmentace provozu s využitím Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	
VRF aware směrovací protokoly, min. OSPF a BGP	
Minimálně 64 oddělených (nezávislých) směrovacích tabulek	64
Mikrosegmentace provozu s využitím security group tags nebo ekvivalentní funkcionality	
Možnost aplikovat ACL pro jednotlivé security group tags	
QoS classification – ACL, DSCP based	
QoS marking	
QoS Shaping and Policing	
Priority queuing	
Hierarchical QoS	
Application aware Zone-based firewall	
IPS/IDS	
URL Filtering	
Advanced Malware Protection	
Možnost rozšířit o funcionalitu TLS 1.3 proxy	
IPSec AES-GCM-256	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	
Agregovaný šifrovací výkon pro IPSec AES-GCM-256 (IMIX provoz) minimálně 6 Gb/s	6.3 Gb/s
IPSec IKEv2	
Možnost rozšířit směrovač o 1/10GE Ethernet modul s podporou IEEE 802.1AE (GCM-AES-256)	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) včetně možnosti definovat signatury pro vlastní aplikace	
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	
SSHv2	
CLI rozhraní	
Programovatelnost prostřednictvím NETCONF/YANG	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	
Možnost plně integrovat směrovač do SD-WAN infrastruktury, jejíž funkční specifikace je uvedena ve specifikaci Katalogového listu SL03 - Služba Provoz centrálního automatizovaného managementu MSpWAN v oblasti Centrálného automatizovaného managementu Routerů MSpWAN	

2 Identifikace firewallu

Výrobce	**Palo Alto Networks**
Obchodní název	**Palo Alto Networks PA-1420**
Model	**PA-1420**
Part-number	**PAN-PA-1420**

Požadované funkcionality a vlastnosti firewallu

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Zařízení typu next generation firewall ve formě fyzické HW appliance	
Součástí dodávky je firewall, jeho licenční pokrytí a podpora/maintenance výrobce nabízeného řešení.	
Režim podpory výrobce nabízeného řešení je vyžadován minimálně v rozsahu 24/7, NBD	
Řešení se umístilo v posledních 6 letech (2018-2023) alespoň jednou v kvadrantu "leaders" v hodnocení Gartner Magic Quadrant for Network Firewalls	
Uchazeč uvede název výrobce řešení a specifikace nabízeného modelu, včetně výpisu všech konkrétních modulů a licencí, které jsou součástí nabídky	
Nabízené řešení je jako celek tvořeno komponenty jednoho výrobce, včetně používaných signatur, databází a zastřešeno jednotnou podporou výrobce.	
Modul pro zpracování dat musí být v architektuře firewallu oddělen alespoň na úrovni CPU jader od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému negativnímu ovlivnění. Pokud je konfigurace odděleného managementu konfigurovatelná a má dopad na výkonové parametry, je nutno toto zohlednit pro splnění požadavků na propustnost	
Zadavatel vzhledem k požadované maximální úrovni zabezpečení síťového provozu vyžaduje kompletní inspekci veškerého síťového provozu s využitím komplexních detekcí na úrovni IPS, AV, DNS, URL, zero day útoků. Využívá-li nabízená technologie optimalizaci výkonostních parametrů s využitím funkcí mají negativní či kompromisní dopad na uroveň bezpečnostní kontroly síťového provozu, nelze je při plnění výkonostních parametrů uvažovat. Jedná se například o kontrolu pouze vybraných částí/vzorků provozu.	
Všechny výkonostní parametry musí být uvedeny v real world mix paketech, tzv. "application mix"	
Firewall musí obsahovat minimálně 1 dedikovaný port RJ45 1Gb/s pro správu	1Gb/s RJ45 OOBM, RJ-45 consolový port, USB
Propustnost FW při plné aplikační kontrole pro IMIX provoz a zapnutí všech dostupných signatur a kontrol IPS a AV, URL, DNS, IoT, SSH inspekci, sandboxingu a zapnutém logování minimálně 5 Gb/s (app mix)	5,6 Gb/s
Minimálně 1 350 000 současných spojení	1 400 000
Minimální 120 000 nových spojení za sekundu	140 000
Zařízení je rozměrově kompatibilní s 19" rozvaděčem, maximální výška 1U	
Firewall obsahuje minimálně 8 datových portů o rychlosti 1Gbps (fyzické metalické nebo SFP) 8 datových portů o rychlosti 10Gbps (SFP+)	4x 1Gb/s RJ45 8x 1/2,5/5G RJ45 2x 1Gb/s SFP 8x 1/10Gb/s SFP+
Firewall musí podporovat virtuální kontexty	
Součástí dodávky je příslušenství pro montáž do racku ve formě ližin či pevného ukotvení	
Firewall musí plně podporovat IPv4 i IPv6	
Firewall musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64
Firewall musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)
Firewall musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)
Firewall musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směrování.
Firewall musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směrování
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel
Firewall musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let
Firewall musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury sítě
Firewall musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů
Firewall musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty
Firewall musí obsahovat předdefinované threshholdy pro známé aplikační kategorie
Firewall musí mít schopnost provádět FEC (Forward Error Correction)
Firewall musí mít schopnost provádět per-application split tunneling
Firewall musí podporovat kompletní správu z centrálního prvku
Firewall musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu všech síťových a bezpečnostních funkcí v případě výpadku centrálního management prvku
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management prvku
Připojení ke GUI musí podporovat šifrování TLSv1.3
GUI musí obsahovat offline kontextovou nápovědu.
Firewall musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování
Firewall musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování
Firewall musí umožňovat automatickou konfiguraci použitím konfiguračních šablon na připojeném USB flash disku
Firewall musí podporovat možnost dodání předkonfigurovaného zařízení výrobcem pro bezobslužnou konfiguraci pomocí ZTP.
Firewall musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát
Firewall musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu
Firewall musí podporovat nativní nástroj pro odchycení provozu
Firewall musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí vlastního firewallu
Firewall s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz
Firewall musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla
Definovaná aplikace musí představovat "match kritérium" při policy lookup
Firewall musí podporovat identifikaci aplikací napříč všemi porty/protokoly
Firewall musí podporovat identifikaci aplikací na nestandardních portech
Identifikace aplikace musí probíhat přímo ve firewallu
Firewall musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping
Firewall musí podporovat řízení neznámého provozu
Firewall musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla
Uživatelská identita musí představovat "match kritérium" při policy lookup
Firewall musí umožňovat automatický přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček
Firewall musí podporovat kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná
Firewall podporuje dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům
Firewall podporuje dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru
Dešifrovaný provoz lze definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita
Firewall podporuje OCSP (Online Certificate Status Protocol) pro kontrolu platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy
Firewall podporuje dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
Firewall musí poskytovat možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)
Firewall musí podporovat prioritizaci provozu na základě DSCP
Firewall musí podporovat prioritizaci provozu na základě Identifikované aplikace
Firewall musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita
Firewall musí obsahovat lokální úložiště logů
Firewall musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI
Firewall musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL
Firewall musí podporovat přeposílání logů na zařízení třetích stran
Firewall musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla
Firewall musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní Firewall
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB
Sandbox systém musí být od stejného výrobce jako je firewall, ale nemusí být HW součástí NGFW
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro firewall, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní firewallu

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Aktualizace zero-day signatur musí být instalována do firewallu v reálnem čase, čili s nulovou prodlevou
Firewall musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod
Firewall musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu
Firewall musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky
Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí
Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita
Sandbox musí rozpoznat, které závislosti malware potřebuje k tomu, aby se spustil a umí je nasimulovat
Firewall musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu
Firewall musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve Firewall. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla
Firewall musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve firewallu. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB
Firewall musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci
Firewall musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů. Firewall musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů
Firewall musí podporovat import SNORT signatur
Firewall musí pro přístup ke kritickým aplikacím poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci. Tato vlastnost musí být konfigurovatelná na úrovni bezpečnostního pravidla
Firewall musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu
Firewall musí poskytovat funkci k ochraně proti tzv. drive-by downloadům. Způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vratí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane
Firewall musí umět zabránit neznámým injekčním útokům jako je SQL a Command Injection útoky pomocí strojového učení
Firewall musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase
Firewall musí umět rozpoznat komunikaci ukrytou v DoH (DNS-over-HTTPS) požadavcích a aplikovat potřebná DNS bezpečnostní pravidla v reálném čase
Firewall musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.
Firewall musí umožnit detekci a kategorizaci zcizených či napadených domén a zneužití DNS v reálném čase pomocí strojového učení přímo na firewallu nebo pomocí cloudové služby
Podpora post-kvantového šifrování minimálně v rámci IKEv2 a IPsec. Firewall musí podporovat výměnu a vytváření hybridních klíčů založených na RFC 9242 a RFC 9370.
Firewall musí obsahovat nativní podporu pro využívání databáze URL
URL databáze musí být od stejného výrobce jako je firewall
Firewall musí být schopen použít URL kategorii v definici bezpečnostního pravidla
Firewall musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL
Firewall musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní firewallu bez nutnosti kontaktování technické podpory

3 Identifikace switche

Výrobce	**Cisco**
Obchodní název	**Catalyst 9200 24-port data only, Network Advantage**
Model	**C9200-24T-A**
Part-number	**C9200-24T-A**

Požadované funkcionality a vlastnosti switche

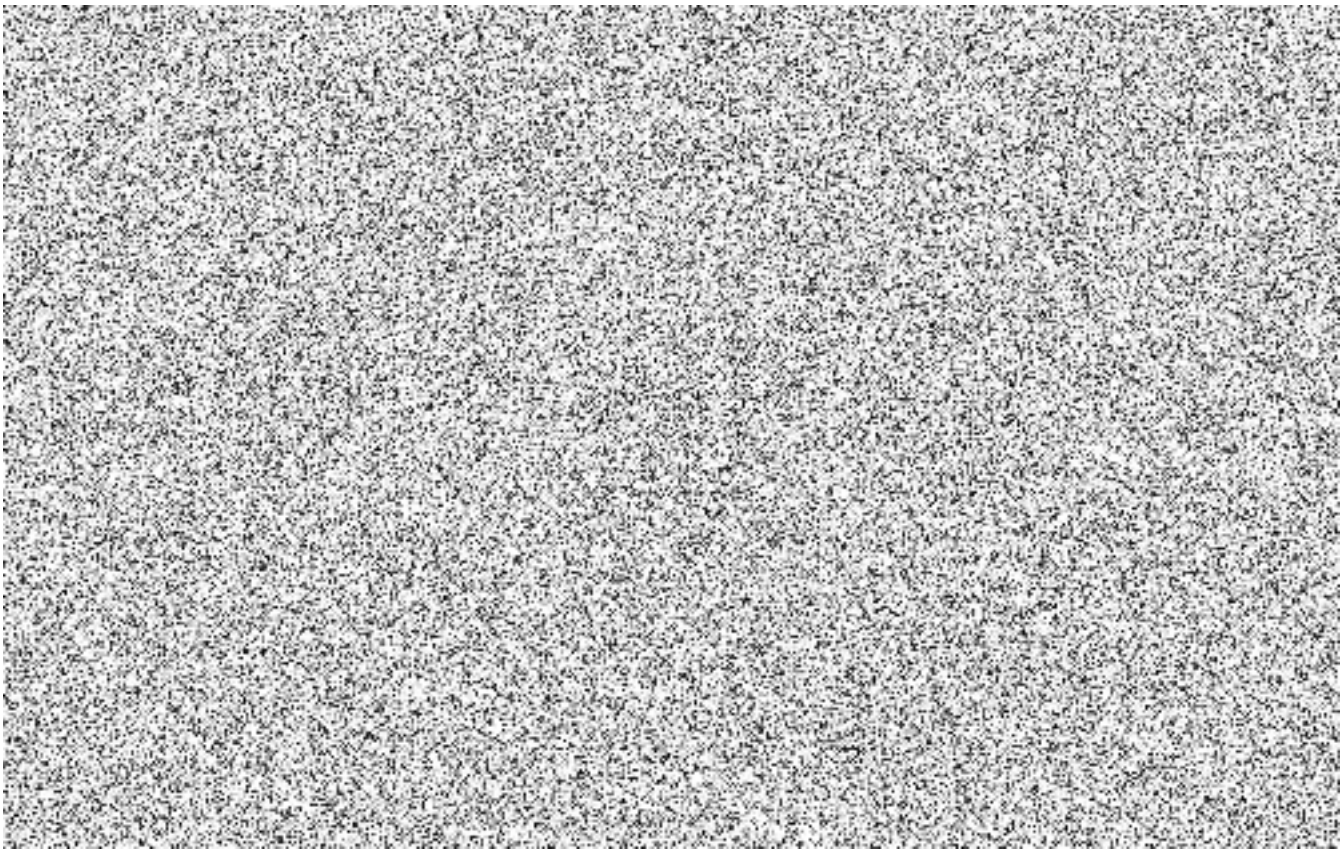
Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
L2/L3 přepínač	
Stohovatelný formát přepínače	
Kapacita sběrnice stohu minimálně 160 Gb/s	160 Gb/s

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Kapacita přepínání minimálně 128 Gb/s	128 Gb/s
Paketová kapacita minimálně 90Mp/s	95 Mp/s
Stateful Switch Over v rámci stohu	
Velikost zařízení 1RU	
Velikost sdíleného systémového bufferu minimálně 6MB	6MB
Redundatní větráky	
Redundatní vyměnitelné větráky	
Možnost instalovat interní redundantní napájecí zdroj	
Minimálně 8 zařízení ve stohu	8
Minimálně 2 dedikované stohovací porty	2
Možnost stohování přes dedikované porty, bez snížení počtu použitelných ethernetových portů	
Minimálně 24 portů 10/100/1000 Base-TX	24
Volitelný modul s uplinkovými porty	
Minimálně 4 Uplinkové porty s rychlostí 1/10GE s volitelným rozhraním SFP+	4
Minimálně 4 Uplinkové porty 100/1000 MB/s s volitelným rozhraním SFP	4
Velikost MAC address tabulky minimálně 32 000 MAC address	32 000
Minimálně 4 000 IPv4 routes	4 000
Minimálně 2 000 IPv6 routes	2 000
Minimálně 1 600 konfigurovatelných security ACL	1 600
IEEE 802.3ad (Link Aggregation)	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	
Minimálně 8 linek jako součást Link Aggregation Group trunku	
Minimálně 48 konfigurovatelných Link Aggregation Group trunků	48
IEEE 802.1Q	
Minimálně 1 000 aktivních VLAN	1000
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	
RADIUS CoA	
Podpora instance spanning-tree protokolu per VLAN	
IEEE 802.1w - Rapid Spanning Tree Protocol	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Podpora Jumbo rámců (minimálně o veliskoti 9 198 bytes)	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	
Směrování protokolů IPv4 a IPv6 v hardware	
RIP, EIGRP Stub, OSPFv2; OSPFv3 - minimálně 1000 Routes	
OSPFv2; OSPFv3	
ISIS	
IP Multicast (PIM SSM, PIM SM)	
Virtualizace směrovacích tabulek - např. Virtual Routing and For Warding (VRF)	
HSRP	
VRRP	
Reverse path check (uRPF) pro IPv4 i IPv6	
IGMPv2, IGMPv3	
IGMP snooping	
MLD snooping	
Minimálně 8 HW QoS front	8
QoS classification – ACL, DSCP, CoS based	
QoS marking - DSCP, CoS	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	
QoS Policing	
QoS-minmálně 2 Hierarchical QoS	2
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	
Možnost definovat povolené MAC adresy na portu	
PACL, VACL	
Paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny	
IEEE 802.1ae (AES-GCM-128) na uplink portech	
IEEE 802.1ae (AES-GCM-256) na uplink portech	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	
IEEE 802.3az	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikaci (DPI na7.vrstvě OSI modelu dle aplikačních signatur)
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX
Podpora Full Flexible Netflow
SSHv2
CLI rozhraní
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení
Aplikace softwarových záplat, nikoli povyšování celého firmware
Streaming telemetrie prostřednictvím NETCONF/XML
SNMPv2/v3
Podpora network boot (iPXE)
Inventarizovatelnost komponent integrovanou RFID identifikací
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
AVC (NBAR2)
NTPv3 server

Příloha č. 1D – Malé komunikační centrum



Prvky Malého komunikačního centra jsou zapojené neredundantně dle obrázku výše.

Předpokládaná rychlost připojení k Infrastruktuře MSpWAN nepřekročí 1 Gb/s.

1 Identifikace routeru

Výrobce	**Cisco**
Obchodní název	**Cisco Catalyst C8200-1N-4T Router**
Model	**C8200-1N-4T**
Part-number	**C8200-1N-4T**

Požadované funkcionality a vlastnosti routeru

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Typ zařízení: Směrovač	
Modulární formát zařízení	
Počet portů GigabitEthernet: minimálně 2x 10/100/1000Base-T	2
Minimálně 2 porty GigabitEthernet s volitelným fyzickým rozhraním typu SFP	2
AC napájecí zdroj 230V	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Min. 2 volné sloty pro rozšiřující komunikační moduly	
Možnost rozšířit směrovač o Wireless WAN modul s rozhraním 5G/LTE s následujícími parametry: 5G (Sub 6GHz) LTE category 20 Podpora dual SIM	 Ano Ano Ano
Propustnost systému minimálně 3,5 Gb/s	3,8 Gb/s
Podpora jumbo frames (minimálně veikosti 9 200 bytes)	Ano
OSPFv2, OSPFv3	
BGPv4, MP-BGP	
First Hop Redundancy Protokol (VRRP nebo HSRP)	
Interface tracker pro FHRP	
GRE (Generic Routing Encapsulation)	
Policy-based routing podle ACL	
IP Multicast (PIM SSM, PIM ASM)	
IGMPv2, IGMPv3	
DHCP server pro IPv4	
DHCP relay pro IPv4	
Makrosegmentace provozu s využitím Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	
VRF aware směrovací protokoly, min. OSPF a BGP	
Minimálně 64 oddělených (nezávislých) směrovacích tabulek	64
Mikrosegmentace provozu s využitím security group tags nebo ekvivalentní funkcionality	
Možnost aplikovat ACL pro jednotlivé security group tags	
QoS classification – ACL, DSCP based	
QoS marking	
QoS Shaping and Policing	
Priority queuing	
Hierarchical QoS	
Application aware Zone-based firewall	
IPS/IDS	
URL Filtering	
Advanced Malware Protection	
Možnost rozšířit o funcionalitu TLS 1.3 proxy	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
IPSec AES-GCM-256	
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	
Agregovaný šifrovací výkon pro IPSec AES-GCM-256 (IMIX provoz) minimálně 900 Mb/s	900 Mb/s
IPSec IKEv2	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) včetně možnosti definovat signatury pro vlastní aplikace	
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	
SSHv2	
CLI rozhraní	
Programovatelnost prostřednictvím NETCONF/YANG	
SNMPv2/v3	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	
NTPv3 server	
Možnost plně integrovat směrovač do SD-WAN infrastruktury, jejíž funkční specifikace je uvedena ve specifikaci Katalogového listu SL03 - Služba Provoz centrálního automatizovaného managementu MSpWAN v oblasti Centrálného automatizovaného managementu Routerů MSpWAN	

2 Identifikace firewallu

Výrobce	**Palo Alto Networks**
Obchodní název	**Palo Alto Networks PA-440**
Model	**PA-440**
Part-number	**PAN-PA-440**

Požadované funkcionality a vlastnosti firewallu

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Zařízení typu next generation firewall ve formě fyzické HW appliance	
Součástí dodávky je firewall, jeho licenční pokrytí a podpora/maintenance výrobce nabízeného řešení.	
Režim podpory výrobce nabízeného řešení je vyžadován minimálně v rozsahu 24/7, NBD	
Řešení se umístilo v posledních 6 letech (2018-2023) alespoň jednou v kvadrantu "leaders" v hodnocení Gartner Magic Quadrant for Network Firewalls	
Uchazeč uvede název výrobce řešení a specifikace nabízeného modelu, včetně výpisu všech konkrétních modulů a licencí, které jsou součástí nabídky	
Nabízené řešení je jako celek tvořeno komponenty jednoho výrobce, včetně používaných signatur, databází a zastřešeno jednotnou podporou výrobce.	
Modul pro zpracování dat musí být v architektuře firewallu oddělen alespoň na úrovni CPU jader od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému negativnímu ovlivnění. Pokud je konfigurace odděleného managementu konfigurovatelná a má dopad na výkonové parametry, je nutno toto zohlednit pro splnění požadavků na propustnost	
Zadavatel vzhledem k požadované maximální úrovni zabezpečení síťového provozu vyžaduje kompletní inspekci veškerého síťového provozu s využitím komplexních detekcí na úrovni IPS, AV, DNS, URL, zero day útoků. Využívá-li nabízená technologie optimalizaci výkonostních parametrů s využitím funkcí mají negativní či kompromisní dopad na uroveň bezpečnostní kontroly síťového provozu, nelze je při plnění výkonostních parametrů uvažovat. Jedná se například o kontrolu pouze vybraných částí/vzorků provozu.	
Všechny výkonostní parametry musí být uvedeny v real world mix paketech, tzv. "application mix"	
Firewall musí obsahovat minimálně 1 dedikovaný port RJ45 pro správu o rychlosti 1Gb/s	1Gb/s RJ45 OOBM, RJ-45 consolový port, USB
Propustnost FW při plné aplikační kontrole pro IMIX provoz a zapnutí všech dostupných signatur a kontrol IPS a AV, URL, DNS, IoT, SSH inspekci, sandboxingu a zapnutém logování minimálně 1 Gb/s (app mix)	1,2 Gb/s
Minimálně 200 000 současných spojení	200 000
Minimálně 30 000 nových spojení za sekundu	34 000
Zařízení je rozměrově kompatibilní s 19" rozvaděčem, maximální výška 1U	1U
Firewall obsahuje minimálně 8 datových portů rychlosti 1Gbps (fyzické metalické)	8x 1Gb/s RJ45
Firewall musí podporovat virtuální kontexty	
Součástí dodávky je příslušenství pro montáž do racku ve formě ližin či pevného ukotvení	
Firewall musí plně podporovat IPv4 i IPv6	
Firewall musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	
Firewall musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	
Firewall musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)	
Firewall musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směrování.
Firewall musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směrování
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel
Firewall musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let
Firewall musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury sítě
Firewall musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů
Firewall musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty
Firewall musí obsahovat předdefinované threshholdy pro známé aplikační kategorie
Firewall musí mít schopnost provádět FEC (Forward Error Correction)
Firewall musí mít schopnost provádět per-application split tunneling
Firewall musí podporovat kompletní správu z centrálního prvku
Firewall musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu všech síťových a bezpečnostních funkcí v případě výpadku centrálního management prvku
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management prvku
Připojení ke GUI musí podporovat šifrování TLSv1.3
GUI musí obsahovat offline kontextovou nápovědu.
Firewall musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování
Firewall musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování
Firewall musí umožňovat automatickou konfiguraci použitím konfiguračních šablon na připojeném USB flash disku
Firewall musí podporovat možnost dodání předkonfigurovaného zařízení výrobcem pro bezobslužnou konfiguraci pomocí ZTP.
Firewall musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát
Firewall musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu
Firewall musí podporovat nativní nástroj pro odchycení provozu
Firewall musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)
Firewall management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí vlastního firewallu

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz
Firewall musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla
Definovaná aplikace musí představovat "match kritérium" při policy lookup
Firewall musí podporovat identifikaci aplikací napříč všemi porty/protokoly
Firewall musí podporovat identifikaci aplikací na nestandardních portech
Identifikace aplikace musí probíhat přímo ve firewallu
Firewall musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping
Firewall musí podporovat řízení neznámého provozu
Firewall musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla
Uživatelská identita musí představovat "match kritérium" při policy lookup
Firewall musí umožňovat automatický přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)
Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček
Firewall musí podporovat kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall podporuje dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům
Firewall podporuje dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru
Dešifrovaný provoz lze definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita
Firewall podporuje OCSP (Online Certificate Status Protocol) pro kontrolu platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy
Firewall podporuje dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
Firewall musí poskytovat možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)
Firewall musí podporovat prioritizaci provozu na základě DSCP
Firewall musí podporovat prioritizaci provozu na základě Identifikované aplikace
Firewall musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita
Firewall musí obsahovat lokální úložiště logů
Firewall musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI
Firewall musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL
Firewall musí podporovat přeposílání logů na zařízení třetích stran
Firewall musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla
Firewall musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní Firewall
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB
Sandbox systém musí být od stejného výrobce jako je firewall, ale nemusí být HW součástí NGFW
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro firewall, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní firewallu
Aktualizace zero-day signatur musí být instalována do firewallu v reálnem čase, čili s nulovou prodlevou
Firewall musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu
Firewall musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky
Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí
Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita
Sandbox musí rozpoznat, které závislosti malware potřebuje k tomu, aby se spustil a umí je nasimulovat
Firewall musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu
Firewall musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve Firewall. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla
Firewall musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve firewallu. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB
Firewall musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Firewall musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci
Firewall musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů. Firewall musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů
Firewall musí podporovat import SNORT signatur
Firewall musí pro přístup ke kritickým aplikacím poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci. Tato vlastnost musí být konfigurovatelná na úrovní bezpečnostního pravidla
Firewall musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu
Firewall musí poskytovat funkci k ochraně proti tzv. drive-by downloadům. Způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru
Firewall musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vratí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane
Firewall musí umět zabránit neznámým injekčním útokům jako je SQL a Command Injection útoky pomocí strojového učení

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
Firewall musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase
Firewall musí umět rozpoznat komunikaci ukrytou v DoH (DNS-over-HTTPS) požadavcích a aplikovat potřebná DNS bezpečnostní pravidla v reálném čase
Firewall musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.
Firewall musí umožnit detekci a kategorizaci zcizených či napadených domén a zneužití DNS v reálném čase pomocí strojového učení přímo na firewallu nebo pomocí cloudové služby
Podpora post-kvantového šifrování minimálně v rámci IKEv2 a IPsec. Firewall musí podporovat výměnu a vytváření hybridních klíčů založených na RFC 9242 a RFC 9370.
Firewall musí obsahovat nativní podporu pro využívání databáze URL
URL databáze musí být od stejného výrobce jako je firewall
Firewall musí být schopen použít URL kategorii v definici bezpečnostního pravidla
Firewall musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL
Firewall musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní firewallu bez nutnosti kontaktování technické podpory

3 Identifikace switche

Výrobce	**Cisco**
Obchodní název	**Catalyst 9000 Compact Switch 12 Ports, Data Only, Adv**
Model	**C9200CX-12T-2X2G-A**
Part-number	**C9200CX-12T-2X2G-A**

Požadované funkcionality a vlastnosti switche

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
L2/L3 přepínače	
kompaktní formát přepínače	
Kapacita přepínání minimálně 70 Gb/s	70 Gb/s
Paketová kapacita minimálně 52 mp/s	52 Mp/s
Velikost sdíleného systémového bufferu minimálně 6 MB	6 MB
Bezvětrákové (Fanless) provedení	
Externí napájecí AC zdroj požadován	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
Minimálně 12 portů 10/100/1000 Base-TX	12
Minimálně 2 Uplinkové metalické porty 10/100/1000 Mb/s RJ45	2
Minimálně 2 Uplinkové porty 1/10 Gb/s volitelným rozhraním SFP+	2
Velikost MAC address tabulky minmálně 32 000 MAC address	32 000
Minimáně 4 000 IPv4 routes	4 000
Minimálně 2 000 IPv6 routes	2 000
Minimálně 1 600 konfigurovatelných security ACL	1 600
IEEE 802.3ad (Link Aggregation)	
Minimálně 8 linek jako součást Link Aggregation Group trunku	
Minimální 48 konfigurovatelných Link Aggregation Group trunků	48
IEEE 802.1Q	
Minimálně 512 aktivních VLAN	512
IEEE 802.1x	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	
RADIUS CoA	
Podpora instance spanning-tree protokolu per VLAN	
IEEE 802.1w - Rapid Spanning Tree Protocol	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	
Podpora Jumbo rámců (minimálně velikosti 9 198 bytes)	9 198
Detekce protilehlého zařízení (např. CDP nebo LLDP)	
Směrování protokolů IPv4 a IPv6 v hardware	
RIP, EIGRP Stub, OSPFv2; OSPFv3 - minimálně 1000 Routes	
OSPFv2; OSPFv3	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	
ISIS	
IP Multicast (PIM SSM, PIM SM)	
Virtualizace směrovacích tabulek - např. Virtual Routing and For Warding (VRF)	
LISP	
VXLAN	
BGP	
HSRP	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti	
VRRP	
Reverse path check (uRPF) pro IPv4 i IPv6	
IGMPv2, IGMPv3	
IGMP snooping	
MLD snooping	
Minimálně 8 HW QoS front	8
QoS classification – ACL, DSCP, CoS based	
QoS marking - DSCP, CoS	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	
QoS Policing	
QoS-minimálně 2 úrovně Hierarchical QoS	2
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	
Možnost definovat povolené MAC adresy na portu	
PACL, VACL	
Paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny	
IEEE 802.1ae (AES-GCM-128) na uplink portech	
IEEE 802.1ae (AES-GCM-256) na uplink portech	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	
IEEE 802.3az	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikaci (DPI na7.vrstvě OSI modelu dle aplikačních signatur)	
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	
Podpora Full Flexible Netflow	

Požadovaná funkcionalita/vlastnost a způsob splnění požadované funkcionality/vlastnosti
SSHv2
CLI rozhraní
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení
Aplikace softwarových záplat, nikoli povyšování celého firmware
Streaming telemetrie prostřednictvím NETCONF/XML
SNMPv2/v3
Podpora network boot (iPXE)
Inventarizovatelnost komponent integrovanou RFID identifikací
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
AVC (NBAR2)
NTPv3 server

Příloha č. 2 – Úroveň servisních služeb (SLA)

1 Základní pojmy a definice

1. **Oznamovatel** – Pracovník Objednatele nebo organizační složky Objednatele, který nahlašuje incident nebo požadavek Poskytovateli prostřednictvím ServiceDesku.
2. **Incident** – Jakýkoliv nestandardní stav (závada, porucha, nedostupnost apod.), který vznikne neplánovaně nebo neočekávaně při provozu Infrastruktury MSpWAN.
3. **Požadavek** – Plánovaná nebo požadovaná aktivita při provozu Infrastruktury MSpWAN.
4. **ServiceDesk** – obecné označení procesů a aktivit Poskytovatele realizovaných za účelem zajištění provozu Infrastruktury MSpWAN a poskytování Služeb Infrastruktury MSpWAN.
5. **ServiceDesk systém** – Konkrétní softwarový nástroj Poskytovatele určený k nahlašování a evidenci incidentů nebo požadavků pracovníky Objednatele nebo organizační složky Objednatele.

   ServiceDesk systém musí být dostupný oprávněným osobám Objednatele, oprávněným osobám organizačních složek Objednatele, jakož i dalším osobám, které určí Objednatel.
6. **Řešitel** – Pracovník Poskytovatele řešící incident nebo požadavek v ServiceDesku.
7. **Provozní doba** – Časové vymezení garantované funkčnosti ServiceDesk.
8. **Reakční doba na nahlášení incidentu/zadání požadavku** (RESPONSE TIME) – Časový úsek mezi nahlášením incidentu/požadavku Oznamovatelem a první reakcí Řešitele.
9. **Doba vyřešení incidentu** (FIX TIME INCIDENTU) – Časový úsek od nahlášení incidentu Oznamovatelem do vyřešení incidentu.
10. **Doba vyřešení požadavku** (FIX TIME POŽADAVKU) – Časový úsek od nahlášení požadavku Oznamovatelem do jeho vyřešení.

2 Dostupnost Infrastruktury MSpWAN a Služeb Infrastruktury MSpWAN

Poskytovatel je povinen bezpodmínečně zajistit po celou dobu účinnosti Smlouvy dostupnost Infrastruktury MSpWAN a Služeb Infrastruktury MSpWAN minimálně 99,99 %

3 Prioritizace incidentů a požadavků

Oznamovatel při stanovení priority incidentu vychází ze závažnosti a dopadu incidentu.

Závažnost může být:

- **Nízká** – incident neomezuje při práci, ale obtěžuje
- **Střední** – incident omezuje při práci, ale je k dispozici náhradní řešení
- **Vážná/Vysoká** – incident omezuje v práci a není k dispozici náhradní řešení
- **Kritická/Urgentní** – incident znemožňuje práci

Dopad incidentu může být na:

- **Jednoho uživatele** – omezení práce jednoho uživatele a je pravděpodobné, že další uživatelé nebudou ovlivněni;
- **Několik uživatelů** – omezení práce několika uživatelů (např. menší skupiny uživatelů se specifickými oprávněními nebo specifickou rolí apod.), ale většina pracovníků Objednatele/organizační složky Objednatele může pracovat
- **Mnoho uživatelů** – typicky, ale nejen, výpadek Služeb Infrastruktury MSpWAN, který postihne organizační složku Objednatele apod.
- **Všechny uživatele** – typicky např. výpadek všech Služeb Infrastruktury MSpWAN apod.

Výsledná priorita je určena dle schématu:

Závažnost	**Dopad**			
	Jednoho uživatele	**Několik uživatelů**	**Mnoho uživatelů**	**Všechny uživatele**
Nízká	Priorita P4 (nízká)	Priorita P4 (nízká)	Priorita P3 (střední)	Priorita P3 (střední)
Střední	Priorita P4 (nízká)	Priorita P3 (střední)	Priorita P3 (střední)	Priorita P2 (vysoká)
Vážná	Priorita P4 (nízká)	Priorita P3 (střední)	Priorita P2 (vysoká)	Priorita P1 (urgentní)
Kritická	Priorita P3 (střední)	Priorita P2 (vysoká)	Priorita P2 (vysoká)	Priorita P1 (urgentní)

Obdobně postupuje Oznamovatel postupuje při stanovení priority požadavku, pouze přihlíží k závažnosti a dopadům v případě nerealizace požadavku.

Priorita se může v průběhu řešení incidentu nebo požadavku měnit.

4 Způsob hlášení Incidentu/Požadavku

Hlášení incidentu/požadavku je možné:

- prostřednictvím rozhraní ServiceDesk systému dostupného na www adrese:
- e-mailem zaslaným na adresu:
- telefonicky na číslo:

Telefonické hlášení Incidentu/Požadavku smí být použito pouze za situace, kdy není dostupný ServiceDesk systém nebo nelze odeslat e-mail.

Oznamovatel uvede v hlášení:

- Jméno, příjmení, označení organizační složky a kontaktní e-mail a telefon
- Identifikaci lokality a služby, která je incidentem nebo požadavkem dotčená
- Stručný popis incidentu nebo požadavku
- Prioritu incidentu nebo požadavku (případně i dopady a závažnost).

5 Závazné lhůty definující SLA

Provozní doba ServiceDesk: 24x7

Dostupnost ServiceDesk: 99,6%

Do dostupnosti ServiceDesk se nezapočítávají Objednatelem odsouhlasené technickoprovozní odstávky systému (např. z důvodu upgrade apod).

Reakční doba na nahlášení incidentu/zadání požadavku: ..... 30 minut

Doba vyřešení incidentu

- s Prioritou P1 (urgentní) ..... 4 hodiny
- s Prioritou P2 (vysoká) ..... 8 hodin
- s Prioritou P3 (střední) ..... 12 hodin

- s Prioritou P4 (nízká) ..... 24 hodin

U incidentů s Prioritou P3 nebo P4 si může Řešitel dohodnout s Oznamovatelem individuální dobu vyřešení incidentu. Individuální doba vyřešení incidentu musí být prokazatelně odsouhlasená Oznamovatelem (např. e-mailem) a toto musí být uvedeno v ServiceDesk.

Doba vyřešení požadavku

- s Prioritou P1 (urgentní) ..... 4 hodiny
- s Prioritou P2 (vysoká) ..... 12 hodin
- s Prioritou P3 (střední) ..... 24 hodin
- s Prioritou P4 (nízká) ..... 48 hodin

U požadavků s Prioritou P3 nebo P4 si může Řešitel dohodnout s Oznamovatelem individuální dobu vyřešení požadavku. Individuální doba vyřešení požadavku musí být prokazatelně odsouhlasená Oznamovatelem (např. e-mailem) a toto musí být uvedeno v ServiceDesk.

6 Požadavky na ServiceDesk

Objednatel požaduje, aby ServiceDesk **zajišťoval:**

- on-call pohotovostní podporu v režimu 24x7
- single point of contact funkce
- příjem a distribuci incidentů a požadavků
- hlídaní a měření SLA
- zaznamenávání a kategorizaci požadavků na podporu nebo incidenty
- sledovaní stavu a pokroku každého problému až do jeho vyřešení
- předběžnou diagnostiku hlášených problémů
- okamžité řešení jednoduchých problémů nebo eskalaci složitějších problémů na vyšší úroveň podpory
- technickou podporu, v rámci které poskytuje základní rady a řešení pro problémy se softwarem, hardwarem a sítí

Za účelem naplnění požadavků Objednatele na **ServiceDesk je** tento **povinen**:

- rychle reagovat na dotazy uživatelů a požadavky na podporu
- prioritizovat problémy podle naléhavosti a dopadu

- jasně komunikovat s Oznamovateli o stavu jejich požadavků
- poskytovat pravidelné aktualizace o postupu řešení problémů
- používat analytické schopnosti k identifikaci kořenové příčiny problémů
- implementovat efektivní řešení k vyřešení problémů
- eskalovat nevyřešené nebo složité problémy na vyšší úroveň podpory nebo specializované týmy
- dodržovat organizační politiky a postupy
- zajistit ochranu dat a bezpečnost během diagnostiky a podpory
- udržovat záznamy o aktivitách podpory a řešeních
- vytvářet a aktualizovat články znalostní báze a časté dotazy
- vytvářet běžné reporty prováděných prací na měsíční bázi a Ad hoc/pravidelné automatizované reporty generovatelné prostřednictvím aplikačních rozhraní daného zařízení
- evidovat historii požadavků a jejich reporting

7 Základní schéma řešení incidentu (Incident Management)

Aktivita	Stručný popis
1. Identifikace incidentu:	Detekce a hlášení incidentů.
2. Kategorizace:	Klasifikace incidentů pro usnadnění efektivního řízení a hlášení.
3. Prioritizace:	Posouzení naléhavosti a dopadu k určení priority incidentu.
4. Zaznamenání incidentu:	Zaznamenání všech relevantních detailů incidentu do ServiceDesk systému.
5. Počáteční diagnostika:	Provedení předběžného vyšetření k identifikaci známých řešení nebo náhradních postupů.
6. Eskalace:	Eskalace incidentu na vyšší úroveň podpory, pokud není možné jej vyřešit na počáteční úrovni.
7. Vyšetřování a diagnostika:	Podrobné vyšetření za účelem nalezení hlavní příčiny a řešení.
8. Řešení a obnova:	Implementace řešení k obnovení služby.
9. Uzavření:	Potvrzení s uživatelem, že incident byl vyřešen, a uzavření záznamu o incidentu.

8 Základní schéma řešení problému (Problem Management)

Aktivita	Stručný popis
1. Identifikace problému:	Detekce problémů prostřednictvím trendových analýz, přezkumů hlavních incidentů a dalších proaktivních opatření.
2. Kategorizace:	Klasifikace problémů pro usnadnění efektivního řízení a hlášení.
3. Prioritizace:	Posouzení naléhavosti a dopadu k určení priority problému.
4. Zaznamenání problému:	Zaznamenání všech relevantních detailů problému do ServiceDesk systému.
5. Vyšetření a diagnostika:	Provádění analýzy hlavní příčiny k identifikaci základní příčiny problému.
6. Implementace náhradního řešení:	Vývoj a implementace dočasných řešení ke snížení dopadu problému.
7. Záznam známé chyby:	Dokumentování problému a náhradního postupu jako známé chyby.
8. Řešení:	Implementace trvalého řešení k odstranění problému.
9. Uzavření problému:	Zajištění úplného vyřešení problému a uzavření záznamu o problému.
10. Přezkum hlavního problému:	Přezkoumání hlavních problémů za účelem získání poznatků a zlepšení budoucích aktivit řízení problémů.

9 Základní schéma změnového řízení (Change Management)

Aktivita	Stručný popis
1. Požadavek na změnu:	**Zaznamenání:** Změna začíná zaznamenáním formálního požadavku na změnu, který obsahuje podrobné informace o navrhované změně.
	Kategorizace: Požadavek na změnu je klasifikován podle typu, priority a rizika změny.
2. Posouzení a schválení změny:	**Technické a obchodní hodnocení:** Posouzení technických a bezpečnostních dopadů změny. To zahrnuje analýzu rizik a přínosů.
	Schválení: Požadavek na změnu je předložen ke schválení změnovému poradnímu výboru nebo jiným odpovědným osobám v závislosti na typu a rozsahu změny.

Aktivita	Stručný popis
3. Plánování změny:	**Plánování:** Detailní plánování změny, včetně časového harmonogramu, zdrojů a kroků potřebných pro implementaci.
	Komunikace: Informování všech zainteresovaných stran o plánované změně a jejím dopadu.
4. Testování a příprava:	**Testování:** Provádění testů, aby se zajistilo, že změna bude fungovat podle očekávání a že neovlivní negativně stávající služby.
	Příprava záložního plánu: Připravení plánu pro případ, že by změna neproběhla podle plánu (rollback plan).
5. Implementace změny:	**Realizace:** Implementace změny podle schváleného plánu.
	Monitorování: Sledování změny během a po její implementaci, aby se zajistilo, že funguje správně.
6. Přezkoumání a uzavření změny:	**Přezkoumání:** Zhodnocení úspěšnosti změny a dokumentace všech zjištěných problémů nebo odchylek.
	Uzavření: Formální uzavření požadavku na změnu, pokud byla změna úspěšně implementována a žádné další akce nejsou potřebné.
7. Dokumentace a zlepšení procesu:	**Dokumentace:** Zaznamenání všech relevantních informací o změně, včetně schválení, testovacích výsledků a závěrečného hodnocení.
	Zlepšení procesu: Analýza získaných zkušeností a návrh zlepšení pro budoucí změny.

Příloha č. 3 – Žádost o zřízení komunikačního centra

Žádost o zřízení komunikačního centra		
Název složky:		
Adresa umístění komunikačního centra		
Žadatel:	*Elektronický podpis*	
Datová linka:		
KIVS ID		
Operátor:		
Kapacita:		
Zakončení (typ konektoru):		
Komunikační centrum:		
Velké (s redundancí)	**Střední** (bez redundance)	**Malé** (bez redundance)
☐	☐	☐
Kontaktní údaje v lokalitě		
Organizační složka:		
Jméno kontaktní osoby:		
Telefon:		
e-mail:		
Souhlas MSp se zřízením komunikačního centra		
Schvalovatel:	*Elektronický podpis*	

V rámci poskytnutí součinnosti je organizační složka povinna zajistit:

- fyzický přístup do místnosti, v které bude instalováno komunikační centrum, případně do místnosti se zakončením datové linky (pokud se jedná o různé místnosti);
- fyzický přístup do místnosti s komunikačním centrem v případě potřeby výměny, řešení poruchy;
- dostatečný prostor v racku pro instalaci
    - velkého komunikačního centra (s redundancí) minimálně 6U (2x Router, 2x Firewall, 2x Switch) a hloubce racku min. 600 mm. Doporučeno je 10U (vždy 1U nad a pod dvojící zařízení) a hloubka racku minimálně 800 mm;
    - střední a malé komunikační centrum (bez redundance) minimálně 3U (1x Router, 1x Firewall, 1x Switch) a hloubce racku min. 600 mm. Doporučeno je 7U (vždy 1U nad a pod zařízením) a hloubka racku minimálně 800 mm;
- napájení v racku včetně UPS pro
    - velké komunikační centrum 6x pozice pro připojení CEE7 zástrčky (2x Router, 2x Firewall, 2x Switch);
    - střední a malé komunikační centrum 3x pozice pro připojení CEE7 zástrčky (1x Router, 1x Firewall, 1x Switch);
- chlazení v racku či místnosti, aby bylo možné provozovat zařízení v souladu s doporučením výrobce (typická hodnota je mezi 15 a 25°C).

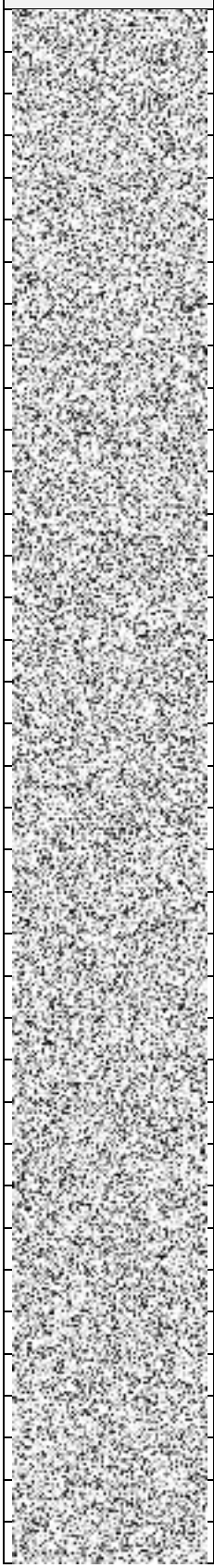
Pokud si organizační složka a Poskytovatel nedohodnou jinak, je Poskytovatel povinen dodat, zprovoznit a napojit do Infrastruktury MSpWAN:

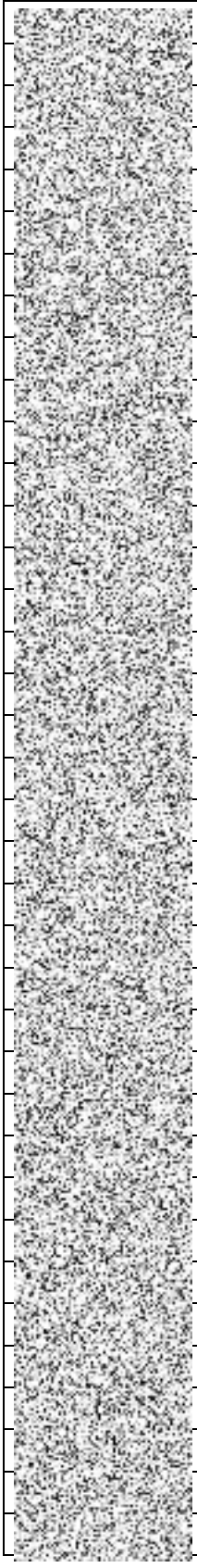
- Velké komunikační centrum do 45 dnů
- Střední nebo Malé komunikační centrum do 30 dnů

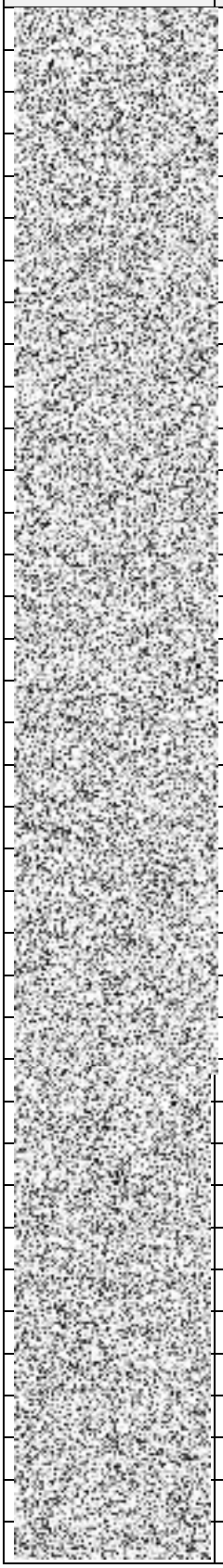
od schválení Žádosti o zřízení komunikačního centra Objednatelem.

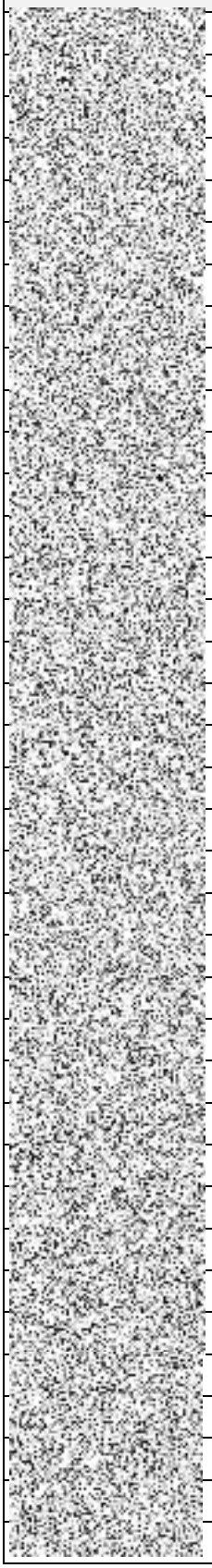
Příloha č. 4 – Seznam a kategorizace Implementačních lokalit

[redacted]	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Praha	Na Děkance 3/1937	Hlavní	10 000
	Praha	28. pluku 29/1533	Hlavní	10 000
	Praha	Spálená 2/6	Velké	1 000
	Praha	náměstí 14. října 9/2188	Velké	300
	Praha	Ovocný trh 14/587	Střední	250
	Praha	Francouzská 19/808	Střední	150
	Praha	Jagellonská 5/1734	Střední	150
	Praha	Hybernská 18/1006	Střední	200
	Praha	Jiráskova /166	Malé	50
	Praha	náměstí Kinských 5/234	Velké	500
	Praha	Husova 11/243	Střední	200
	Praha	Na Poříčí 20/1044	Střední	150
	Praha	Karmelitská 19/377	Střední	140
	Benešov	Masarykovo náměstí /223	Malé	70
	Benešov	Poštovní /2079	Malé	60
	Beroun	Wagnerovo nám. 3/1249	Malé	80
	Kladno	nám. Edvarda Beneše /1997	Střední	150
	Kladno	Pavlisova /2818	Malé	80
	Kolín	Kmochova /144	Malé	100
	Kolín	Politických vězňů /573	Malé	50
	Kutná Hora	náměstí Národního odboje 6/58	Malé	100
	Kutná Hora	Radnická 36/178	Malé	50
	Mělník	Krombholcova 1/264	Malé	100
	Mělník	Vodárenská 1/210	Malé	100
	Mladá Boleslav	náměstí Republiky 11/100	Malé	120
	Mladá Boleslav	S. K. Neumanna /544	Malé	100
	Nymburk	Soudní 10/996	Malé	90
	Nymburk	Boleslavská třída 12/139	Malé	80
	Příbram	Milínská /167	Malé	100
	Příbram	U Nemocnice /89	Malé	100
	Rakovník	Sixtovo náměstí /76	Malé	50
	Rakovník	Na Letné /2175	Malé	50
	České Budějovice	Zátkovo nábř. 2/10	Velké	1 000

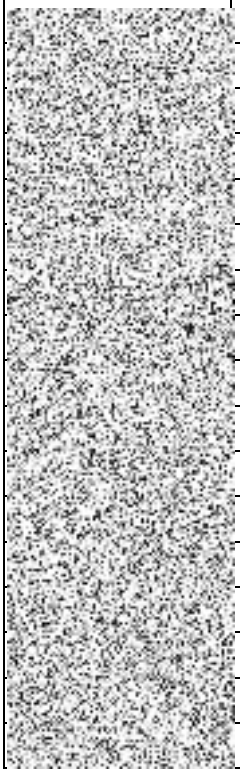
Implementační lokalita ID	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Tábor	Kpt. Jaroše /1851	Velké	500
	Český Krumlov	Linecká /284	Malé	70
	Český Krumlov	Kaplická /162	Malé	50
	Jindřichův Hradec	Klášterská /123	Malé	80
	Jindřichův Hradec	Stará cesta /253	Malé	60
	Pelhřimov	třída Legií /876	Malé	70
	Písek	Velké náměstí 17/121	Malé	100
	Prachatice	Pivovarská /3	Malé	100
	Strakonice	Smetanova /455	Malé	100
	Brno	Jihlavská 12/410	Střední	200
	Hradec Králové	Hradební 7/860	Malé	50
	Hradec Králové	Vážní /903	Malé	50
	Litoměřice	Veitova 1/1888	Malé	50
	Olomouc	Švermova 2/1161	Malé	50
	Praha	Staré náměstí 12/3	Malé	70
	Praha	K šancím 6/50	Malé	50
	Velké Přílepy	U Rybníčku /274	Malé	50
	Teplice	Daliborova stezka /2233	Malé	120
	Bělušice	Bělušice /66	Střední	150
	Břeclav	Za Bankou 3/3087	Malé	50
	Břeclav	Hraniční 223/1303	Malé	50
	Ostrava	Orlovská 35/670	Malé	120
	Horní Slavkov	Hasičská /785	Střední	150
	Jiřice	Ruská cesta /404	Střední	200
	Kuřim	Blanenská 127/1191	Střední	140
	Kynšperk nad Ohří	Zlatá /52	Střední	140
	Mírov	areál věznice /	Malé	120
	Nové Sedlo	/2	Malé	80
	Lubenec	Drahonice /41	Malé	50
	Malé Svatoňovice	Odolov /41	Malé	70
	Opava	Krnovská 70/2771	Malé	50
	Oráčov	Oráčov /159	Střední	140
	Ostrov	Vykmanov /22	Střední	200
	Pardubice	Husova /194	Malé	100
	Dubenec	Dubenec /100	Střední	200
	Lesní Jakubov	Lesní Jakubov /44	Střední	150
	Jablonec nad Nisou	Belgická 11/3765	Malé	120

Implementační lokalita ID	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Světlá nad Sázavou	Rozkoš /990	Střední	200
	Valdice	nám. Míru /55	Střední	250
	Vinařice	Vinařice /245	Střední	200
	Všehrdy	Všehrdy /26	Malé	120
	Stráž pod Ralskem	Máchova /260	Střední	200
	Stráž pod Ralskem	Máchova /200	Střední	200
	Skuteč	Vítězslava Nováka /611	Malé	100
	Radimovice u Želče	Radimovice u Želče /118	Malé	50
	Špindlerův Mlýn	Přední Labská /43	Malé	50
	Plzeň	Veleslavínova 40/21	Velké	1 000
	Plzeň	Veleslavínova 38/27	Střední	MAN PLZ
	Plzeň	Edvarda Beneše 1/1127	Střední	MAN PLZ
	Plzeň	sady 5. května 11/2396	Malé	MAN PLZ
	Plzeň	Klatovská třída 202/652	Malé	MAN PLZ
	Plzeň	Nádražní 7/325	Malé	MAN PLZ
	Plzeň	Klicperova 13/662	Malé	MAN PLZ
	Domažlice	Paroubkova /228	Malé	100
	Domažlice	Komenského /8	Malé	50
	Cheb	Lidická 1/1066	Střední	200
	Karlovy Vary	Moskevská 17/1163	Malé	120
	Karlovy Vary	Jaltská 4/1043	Malé	60
	Klatovy	Dukelská /138	Střední	140
	Rokycany	Jiráskova /67	Malé	60
	Sokolov	Karla Havlíčka Borovského /57	Malé	120
	Sokolov	Karla Havlíčka Borovského /408	Malé	50
	Tachov	náměstí Republiky /71	Malé	60
	Tachov	Václavská /1606	Malé	50
	Ústí nad Labem	Národního odboje 26/1274	Velké	1 000
	Liberec	U Soudu 3/540	Velké	500
	Ústí nad Labem	Dlouhá 12/1	Střední	150
	Ústí nad Labem	Dvořákova 2/3134	Malé	80
	Česká Lípa	Děčínská 2/390	Střední	150
	Česká Lípa	Pod Holým vrchem 22/351	Malé	60
	Děčín	Masarykovo nám. 1/1	Střední	150
	Děčín	Masarykovo nám. 13/97	Malé	80
	Chomutov	Partyzánská /427	Střední	250
	Jablonec nad Nisou	Mírové náměstí 5/494	Malé	90

Implementační lokalita ID	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Jablonec nad Nisou	Liberecká 8/593	Malé	50
	Litoměřice	Na Valech 12/525	Střední	150
	Litoměřice	Žižkova 6/800	Malé	60
	Louny	Sladkovského /1132	Malé	90
	Louny	Pod Nemocnicí /2380	Malé	50
	Most	Moskevská /2	Střední	150
	Most	Václava Řezáče /314	Malé	80
	Teplice	U Soudu /1450	Střední	150
	Teplice	Vrchlického 6/1009	Malé	70
	Hradec Králové	Československé armády 57/218	Střední	250
	Hradec Králové	Zieglerova 1/189	Malé	120
	Hradec Králové	Ignáta Herrmanna 2/227	Střední	200
	Pardubice	Na Třísle /135	Střední	250
	Pardubice	Arnošta z Pardubic /2082	Malé	70
	Havlíčkův Brod	Husova /2895	Malé	80
	Havlíčkův Brod	Štáflova /2003	Malé	50
	Chrudim	Všehrdovo náměstí /45	Malé	80
	Chrudim	Novoměstská /364	Malé	50
	Jičín	Šafaříkova /842	Malé	100
	Náchod	Palachova /1303	Malé	100
	Náchod	Kladská /1092	Malé	50
	Rychnov nad Kněžnou	Svatohavelská /93	Malé	100
	Rychnov nad Kněžnou	Javornická /1501	Malé	60
	Semily	Nádražní /25	Malé	100
	Svitavy	Dimitrovova 33/679	Malé	80
	Svitavy	náměstí Míru 79/196	Malé	50
	Trutnov	Nádražní /106	Malé	100
	Trutnov	Horská /5	Malé	100
	Ústí nad Orlicí	Husova /975	Malé	90
	Ústí nad Orlicí	M. R. Štefanika /980	Malé	50
	Ostrava	Havlíčkovo nábřeží 34/1835	Velké	1 000
	Ostrava	U Soudu 4/6187	Velké	600
	Ostrava	Hrabákova 1/1861	Malé	70
	Olomouc	Studentská 7/1187	Velké	1 000
	Olomouc	Masarykova třída 1/609	Velké	MAN OLC
	Olomouc	17. listopadu 44/909	Střední	MAN OLC
	Olomouc	tř. Svobody 16/685	Malé	MAN OLC

Implementační lokalita ID	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Bruntál	Partyzánská 11/1453	Střední	150
	Krnov	Revoluční 60/965	Malé	50
	Frýdek-Místek	Na Poříčí /3206	Střední	250
	Jeseník	Dukelská 2/761	Střední	150
	Jeseník	Nábřežní 20/290	Malé	70
	Karviná	park Bedřicha Smetany 5/176	Velké	600
	Nový Jičín	Tyršova 3/1010	Střední	200
	Opava	Olomoucká 27/297	Střední	150
	Opava	Lidická 23/257	Malé	70
	Přerov	Smetanova 2/2016	Střední	200
	Šumperk	M. R. Štefánika 12/784	Střední	200
	Vsetín	Horní náměstí /5	Malé	120
	Valašské Meziříčí	Legií /1374	Malé	60
	Praha	Senovážné náměstí 1/995	Střední	200
	Benešov	Poštovní /2079	Malé	50
	Beroun	Politických vězňů 18/20	Malé	50
	Bruntál	Nádražní 20/994	Malé	50
	Břeclav	17. listopadu 1/2995	Malé	120
	České Budějovice	Lannova tř. 63/117	Malé	50
	Český Krumlov	5. května /251	Malé	50
	Děčín	Lázeňská 12/1268	Malé	50
	Rumburk	Náměstí Lužické 2/387	Malé	50
	Frýdek-Místek	Politických obětí /128	Malé	100
	Havlíčkův Brod	Smetanovo náměstí /279	Malé	50
	Hodonín	Národní třída 14/266	Malé	50
	Chomutov	Vikové-Kunětické 2/1968	Malé	100
	Chrudim	Poděbradova /909	Malé	50
	Jablonec nad Nisou	Podhorská 62/564	Malé	60
	Jičín	Balbínova /27	Malé	50
	Jindřichův Hradec	Na Hradbách /43	Malé	50
	Karlovy Vary	Kpt. Jaroše 4/318	Malé	70
	Karviná	Zakladatelská 20/974	Malé	60
	Kladno	náměstí 17. listopadu /2840	Malé	80
	Kolín	Politických vězňů /109	Malé	50
	Liberec	nám. Dr. E. Beneše 26/585	Malé	100
	Louny	Pod Nemocnicí /2381	Malé	50
	Most	Pionýrů 11/2921	Malé	120

Implementační lokalita ID	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Olomouc	Mozartova 4/110	Malé	80
	Opava	Olomoucká 8/9	Malé	70
	Ostrava	Tovární 18/985	Střední	200
	Pardubice	17. listopadu /237	Malé	70
	Pelhřimov	Pražská /127	Malé	50
	Písek	Otakara Ševčíka /1943	Malé	50
	Písek	Samoty /2747	Malé	50
	Prachatice	Hradební /435	Malé	50
	Prostějov	Floriána Nováka 3/5267	Malé	50
	Rakovník	Na Sekyře /2123	Malé	50
	Rokycany	Svazu bojovníků za svobodu /68	Malé	50
	Semily	Bítouchovská /1	Malé	50
	Sokolov	Jednoty /654	Malé	100
	Svitavy	Milady Horákové 10/373	Malé	60
	Tábor	Roháčova /2614	Malé	50
	Tachov	T. G. Masaryka /1326	Malé	50
	Teplice	Husitská 2/1071	Malé	80
	Uherské Hradiště	Protzkarova /1180	Malé	60
	Ústí nad Labem	Velká Hradební 2/484	Malé	120
	Ústí nad Orlicí	Smetanova /43	Malé	50
	Vsetín	Mostecká /303	Malé	70
	Vyškov	Palánek 1/250	Malé	50
	Zlín	Šedesátá /7015	Malé	50
	Žďár nad Sázavou	Komenského 25/1786	Malé	50
	Brno	Rooseveltova 16/648	Velké	2 000
	Brno	Burešova 20/571	Velké	MAN BRN
	Brno	Moravské náměstí 6/611	Velké	MAN BRN
	Brno	Jezuitská 4/585	Velké	MAN BRN
	Brno	Polní 39/994	Střední	MAN BRN
	Brno	Mozartova 3/18	Střední	MAN BRN
	Brno	Husova 15/335	Malé	MAN BRN
	Brno	Moravské náměstí 2/132	Malé	MAN BRN
	Jihlava	třída Legionářů /5277	Velké	300
	Zlín	Dlouhé díly /351	Velké	300
	Blansko	Hybešova 5/2047	Malé	100
	Blansko	Seifertova 9/2025	Malé	50
	Břeclav	Národních hrdinů 11/17	Malé	90

Implementační lokalita ID	Obec	Ulice	Kategorie Komunikačního centra v Implementační lokalitě	Přenosová rychlost [Mb/s]
	Břeclav	U Stadionu 2/1144	Malé	50
	Hodonín	Velkomoravská 4/2269	Malé	90
	Hodonín	Velkomoravská 11/1734	Malé	50
	Kroměříž	náměstí Míru 7/517	Střední	200
	Prostějov	Havlíčkova 16/2936	Malé	80
	Prostějov	Rejskova 14/3018	Malé	50
	Třebíč	Bráfova tř. 57/502	Střední	140
	Uherské Hradiště	Svatováclavská /568	Malé	90
	Uherské Hradiště	Velehradská třída /1217	Malé	50
	Vyškov	Kašíkova 28/314	Malé	70
	Vyškov	Svatopluka Čecha 4/14	Malé	50
	Znojmo	náměstí Republiky 1/585	Střední	200
	Znojmo	Rudoleckého 14/906	Malé	100
	Žďár nad Sázavou	Strojírenská 28/2210	Malé	100
	Praha	Vyšehradská 16/427	Velké	MAN PHA
	Praha	28. pluku 29/1533	Velké	MAN PHA
	Praha	Soudní 1a/1672	Velké	MAN PHA

Příloha č. 5 – Realizační tým

Osoby, jimiž Poskytovatel prokázal splnění kvalifikace:

- **Projektový manažer:**

  Jméno: [redacted]

  Příjmení: [redacted]

  e-mail: [redacted] telefon: [redacted]

  Požadavky:

  - ukončené vysokoškolské vzdělání v magisterském studijním programu;
  - platná certifikace v oblasti projektového řízení (např. PRINCE2 – Foundation nebo PRINCE2 – Practicioner apod.);
  - minimálně 5 let prokazatelné praxe na pozici projektového manažera;
  - znalost českého nebo slovenského jazyka na úrovni rodilého mluvčího, český jazyk písmem.

- **Specialista pro systémy WAN**

  Jméno: [redacted]

  Příjmení: [redacted]

  e-mail: [redacted] telefon: [redacted]

  Požadavky:

  - minimálně ukončené středoškolské vzdělání s maturitou;
  - platná nejvyšší dostupná certifikace výrobce nabízené technologie v oblasti WAN síťových technologií;
  - minimálně 3 roky prokazatelné praxe na pozici IT specialisty v oblasti systémů WAN;
  - znalost českého nebo slovenského jazyka na úrovni rodilého mluvčího.

• **Specialista pro systémy WAN**

Jméno: [redacted]

Příjmení: [redacted]

e-mail: [redacted], telefon: [redacted]

Požadavky:

- minimálně ukončené středoškolské vzdělání s maturitou;

- platná nejvyšší dostupná certifikace výrobce nabízené technologie v oblasti SD WAN

síťových technologií;

- minimálně 3 roky prokazatelné praxe na pozici IT specialisty v oblasti systémů WAN;

- znalost českého nebo slovenského jazyka na úrovni rodilého mluvčího.

- **Specialista na systémy Firewall**

  Jméno: [redacted]

  Příjmení: [redacted]

  e-mail: [redacted] telefon: [redacted]

  Požadavky:

  - minimálně ukončené středoškolské vzdělání s maturitou;
  - platná nejvyšší dostupná certifikace výrobce nabízené technologie Firewall;
  - minimálně 3 roky prokazatelné praxe na pozici IT specialisty v oblasti systémů Firewall;
  - znalost českého nebo slovenského jazyka na úrovni rodilého mluvčího.

- **Solution architekt**

  Jméno:

  Příjmení:

  e-mail: telefon:

  Požadavky:

  - ukončené vysokoškolské vzdělání v magisterském studijním programu;
  - má minimálně 5 let prokazatelné praxe na pozici Solution architekt;
  - znalost českého nebo slovenského jazyka na úrovni rodilého mluvčího.

- **SOC/Pentest architekt**

  Jméno:

  Příjmení:

  e-mail: telefon:

  Požadavky:

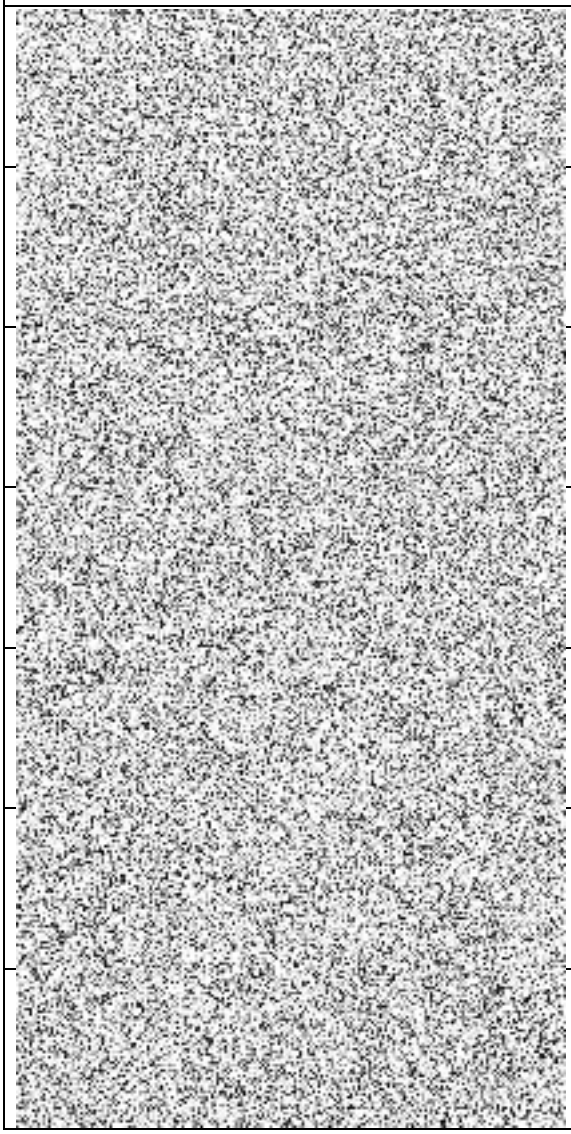
  - ukončené vysokoškolské vzdělání v magisterském studijním programu;
  - minimálně jedna platná certifikace z uvedených: ASP nebo CySA+ nebo CSAE nebo CNSP nebo CSIE nebo CEH nebo CHFI nebo ATT&CK Threat Hunting and Detection Engineering;
  - minimálně 5 let prokazatelné praxe na pozici SOC/Pentest architekt, v rámci které
    - navrhoval a plánoval struktury SOC, včetně hardwarových komponent,
    - prováděl výběr nástrojů pro monitorování, detekci a reakci na bezpečnostní incidenty,
    - nasazoval a konfiguroval bezpečnostní nástroje a systémy a zajišťoval jejich integraci do stávající infrastruktury;
  - znalost českého nebo slovenského jazyka na úrovni rodilého mluvčího.

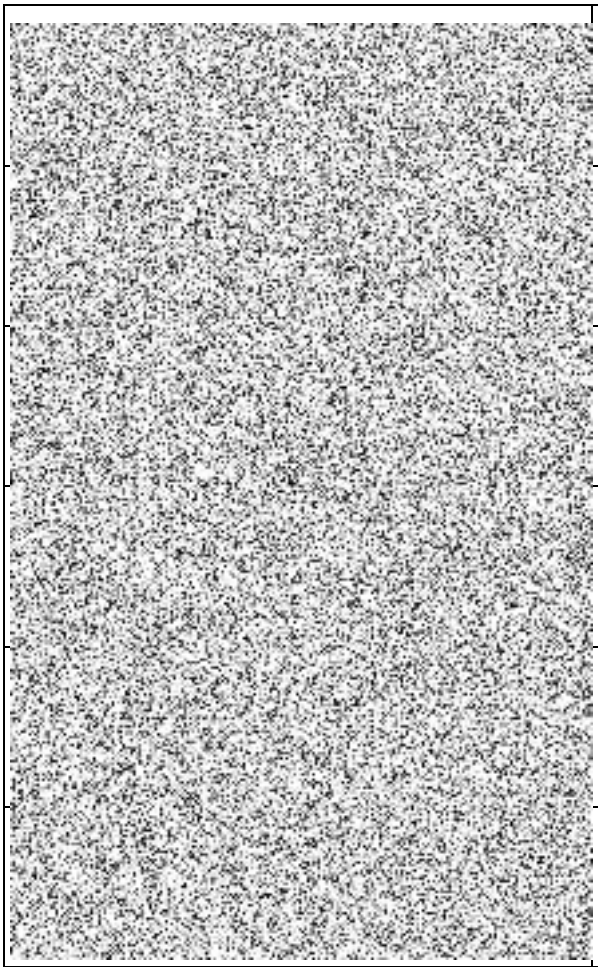
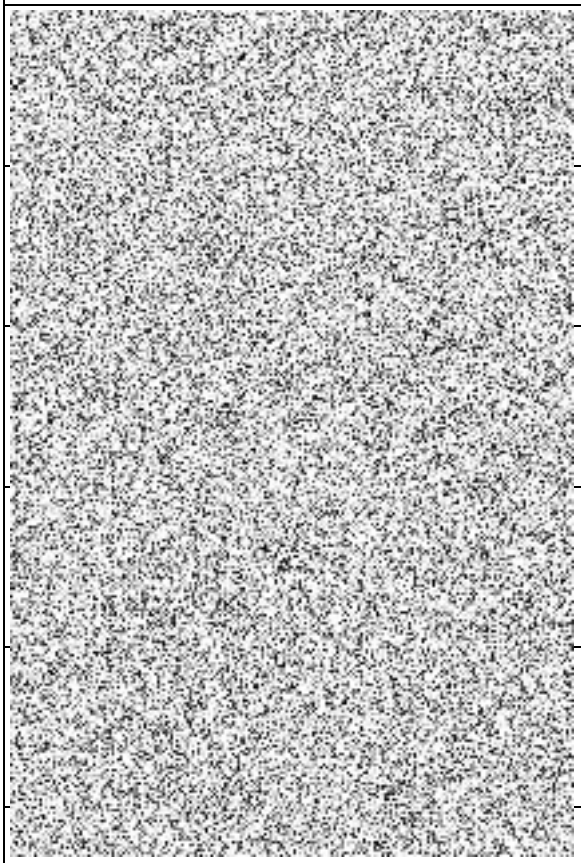
Objednatel vysloveně uvádí, že

- Pracovníci, jimiž Poskytovatel obsadí role „Projektový manažer“, „Solution architekt“ a „SOC/Pentest architekt“ musí být v pracovněprávním vztahu k Poskytovateli.

- Ostatní role můžou být obsazeny osobami, které jsou v pracovněprávním vztahu k Poddodavateli.
- Specialista pro systémy WAN NEMŮŽE být současně v pozici Solution architekt ani SOC/Pentest architekt.
- Specialista Firewall NEMŮŽE být současně v pozici Solution architekt ani SOC/Pentest architekt.

Pracovníci Poskytovatele nebo Poddodavatele, kteří se budou podílet na plnění Smlouvy:

Jméno Příjmení e-mail/telefon	Rozsah činností
	Projektový manažer
	Solution architekt
	Solution architekt
	Specialista pro systémy WAN
	Specialista pro systémy WAN
	SOC/Pentest architekt
	Specialista Compute/Storage

	Specialista Switching/DNA
	Specialista Security/systémy Firewall
	Specialista Security/systémy Firewall
	Specialista Security/systémy Firewall
	Specialista Security/systémy Firewall
	Specialista Security/systémy Firewall
	Specialista Security/bezpečnostní analytik
	Specialista LAN, WAN
	Specialista LAN, WAN
	Specialista LAN, WAN
	SLA služby – nahlašování požadavků, reklamací
	Instalační práce, on-site zásahy v případě

	výměn či troubleshootingu on-site

Vysvětlivky:

- *Do tabulky výše uvede Poskytovatel **všechny** své **pracovníky** (nebo pracovníky Poddodavatele), **kteří se budou přímo podílet na plnění Smlouvy**.*
- *Dodavatel je oprávněn přidat do tabulky další řádky.*

Příloha č. 6 – Vzor měsíčního výkazu

Smlouva o poskytování služeb operátora MSpWAN			
Měsíční výkaz			
Měsíc a rok:		[DOPLNÍ POSKYTOVATEL]	
Počet komunikačních center spravovaných v daném měsíci:			
Hlavní	Velké	Střední	Malé
[DOPLNÍ POSKYTOVATEL]	[DOPLNÍ POSKYTOVATEL]	[DOPLNÍ POSKYTOVATEL]	[DOPLNÍ POSKYTOVATEL]
Cena Služeb v daném měsíci:			
Hlavní	Velké	Střední	Malé
[DOPLNÍ POSKYTOVATEL]	[DOPLNÍ POSKYTOVATEL]	[DOPLNÍ POSKYTOVATEL]	[DOPLNÍ POSKYTOVATEL]
Celková Cena Služeb:		**[DOPLNÍ POSKYTOVATEL]**	
Smluvní pokuty za Degradaci Služeb a za Nedodržení SLA v daném měsíci:			
Pořadí	**Popis**		**Výše slevy**
1	[DOPLNÍ POSKYTOVATEL]		[DOPLNÍ POSKYTOVATEL]
2	[DOPLNÍ POSKYTOVATEL]		[DOPLNÍ POSKYTOVATEL]
3	[DOPLNÍ POSKYTOVATEL]		[DOPLNÍ POSKYTOVATEL]
Smluvní pokuty (dle 16.3 a 16.4 Smlouvy) celkem		**[DOPLNÍ POSKYTOVATEL]**	
Celkem k fakturaci: *(Rozdíl Celkové Cena Služeb a součtu smluvních pokut dle 16.3 a 16.4 Smlouvy)*		**[DOPLNÍ POSKYTOVATEL]**	
Zpracoval:		Akceptoval:	
Elektronický podpis		*Elektronický podpis*	

Příloha č. 7 – Kontaktní osoby

- **Za Objednatele:**

  Jméno: [redacted]

  Příjmení: [redacted], Ing.

  e-mail: [redacted] telefon: [redacted]

- **Za Poskytovatele:**

  Jméno: [redacted]

  Příjmení: [redacted]

  e-mail: [redacted] telefon: [redacted]

Příloha č. 8 – Poddodavatelé

- **Poddodavatel č. 1:**

  Název Poddodavatele: TAKTIK, a.s.

  IČO Poddodavatele: 285 22 869

  Role, kterou bude Poddodavatel zastávat:

  - Poddodavatel služeb v oblasti Security a Datových Center

    Jméno pracovníka Poddodavatele:

    Příjmení pracovníka Poddodavatele:

    e-mail: telefon:

- **Poddodavatel č. 2:**

  Název Poddodavatele: TOTAL SERVICE a.s.

  IČO Poddodavatele: 256 18 067

  Role, kterou bude Poddodavatel zastávat:

  - Poddodavatel služeb v oblasti LAN, WAN

    Jméno pracovníka Poddodavatele:

    Příjmení pracovníka Poddodavatele:

    e-mail: telefon:

- **Poddodavatel č. 3:**

  Název Poddodavatele: GITY, a.s.

  IČO Poddodavatele: 253 02 400

  Role, kterou bude Poddodavatel zastávat:

  - Poddodavatel služeb v oblasti LAN, WAN, Security

    Jméno pracovníka Poddodavatele:

    Příjmení pracovníka Poddodavatele:

    e-mail: telefon: