SPRÁVA ŽELEZNIC

Naše zn. 92605/2025-SŽ-GŘ-O25

Vysvětlení, Změna nebo doplnění zadávací dokumentace č. 3

Sektorová nadlimitní veřejná zakázka dle § 56 zákona č. 134/2016 sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***Zákon***“) na dodávky s názvem:

„**Segmentace sítě**“

Správa železnic, státní organizace (dále jen „***Zadavatel***“) obdržela dne 29. 9. 2025 ve 18:17 hodin žádost o vysvětlení zadávací dokumentace. Zadavatel odpovídá na tuto žádost doručenou k veřejné zakázce následovně:

Dotaz č. 1:

Zadavatel v Příloze č. 2 Zadávací dokumentace (Technická specifikace) v čl. 3.4 Post-implementační a technická podpora v oblasti Post-implementační podpora Dodavatele v odst. 5 uvádí, že služby Helpdesku budou realizovány v souladu se ZOP pro oblast ICT v Režimu 3 (5x8). ZOP pro oblast ICT ale v čl. 10.3 uvádí, že režim 3 je 5x12. Prosíme tedy o vysvětlení, v jakém časovém režimu má být helpdesk poskytován.

Odpověď č. 1:

Zadavatel informuje, že požaduje poskytování Helpdesk v rozsahu (5x8), jak uvádí technická specifikace. Správně je tak odkaz na Režim 4, nikoli na Režim 3, jak správně naznačuje tazatel. Zadavatel s ohledem na uvedené aktualizuje znění Přílohy č. 2 Zadávací dokumentace (Technická specifikace), aby obsahovala správný odkaz ve vztahu k Příloze č. 5 Závazného vzoru smlouvy. Znění upravené Přílohy č. 2 Zadávací dokumentace je Přílohou č. 1 tohoto vysvětlení.

Závěr

Zadavatel sděluje, že s ohledem na povahu shora uvedeného vysvětlení zadávací dokumentace prodlužuje lhůtu pro podání nabídek. Lhůta pro podání nabídek se tak mění a je stanovena na den **13. 10. 2025 do 10:00 hodin**.

Příloha č. 1: Příloha č. 2 - Bližší specifikace předmětu plnění veřejné zakázky (technická specifikace) ve znění změny ze dne 1. 10. 2025

Ing. Dalibor Fajkus
01.10.2025 08:49
Podepsáno
elektronicky

.....
Ing. Dalibor Fajkus
ředitel organizační jednotky
Správa železniční telematiky

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném
Městským soudem v Praze, spisová značka A
48384

Sídlo: Dlážděná 1003/7, 110 00
Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 2 zadávací dokumentace

Technická specifikace

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Obsah

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	Popis
Active Directory	*(AD),* adresářová služba společnosti Microsoft pro správu uživatelů, počítačů a síťových zdrojů v doménovém prostředí.
BGP	*(Border Gateway Protocol)* je protokol pro předávání informací mezi síťovými routery.
CE	*(Customer Edge)* je router na hranici zákaznické sítě v MPLS.
DMI	*(Digital Monitoring Interface)* je funkce diagnostiky SFP modulů.
DHCP	*(Dynamic Host Configuration Protocol*) je protokol pro automatické přidělování IP adres a síťových parametrů koncovým zařízením.
DHCP relay	Mechanismus pro přeposílání DHCP zpráv mezi klienty a DHCP serverem napříč různými sítěmi.
DNS	*(Domain Name System)* je distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu.
EOS	*(End of Sale)* Datum ukončení prodeje.
EOL	*(End of Life)* Datum konce životnosti produktu.
ETC	*(Evidence Technologických Systémů)* Interní systém a konfigurační management (CMDB) zobrazují status sítě.
GDPR	*(General Data Protection Regulation)* nařízení EU o ochraně osobních údajů.
HA	*(High Availability)* je vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku.
HTTPS	*(Hypertext Transfer Protocol Secure)* je šifrovaný protokol pro zabezpečenou komunikaci na webu.
IDS	*(Intrusion Detection System)* Systém detekce průniku používaný v NGFW.
IPFabric	Nástroj pro automatizovanou analýzu a vizualizaci síťové infrastruktury, využívaný pro audit, návrh a správu sítí.

IPS	*(Intrusion Prevention System)* Systém prevence průniku používaný v NGFW.
IPv4	*(Internet Protocol version 4)* je starší verze protokolu IP.
IROP	Integrovaný regionální operační program.
L1 – L3	Vrstvy OSI modelu.
LC	*(Lucent Connector)* typ optického konektoru.
LDAP	*(Lightweight Directory Access Protocol)* je komunikační protokol adresářové služby. Je definován v rámci RFC 4511.
Least Privilege	Bezpečnostní princip, který poskytuje uživatelům a systémům pouze minimální práva nezbytná pro vykonání jejich úkolů.
LLD	*(Low level design),* návrh a specifikace s vyšší mírou podrobnosti.
Malware	Software vytvořený k poškození nebo neoprávněnému přístupu.
MPLS	*(MultiProtocol Label Switching)* Multi-protokolové přepojování podle značek – metoda směrování síťového provozu používaná ve vysokorychlostních telekomunikačních sítích, která pro směrování nepoužívá relativně dlouhé a protokolově závislé síťové adresy, ale krátké značky pevné délky. Standard je definován v RFC 3031.
NBD	*(Next Business Day)* Režim poskytování servisu a podpory.
NGFW	*(Next-Generation Firewall)* Oproti běžným FW nabízí také doplňkové funkce jako AVC, AMP, IPS, IDS, DPI, DLP, TD, IdM a dešifrování a kontrolu TLS/SSL obsahu.
NIS2	*(Network and Information Security Directive 2*) je evropská směrnice o kybernetické bezpečnosti, rozšiřující povinnosti organizací v oblasti ochrany sítí a informačních systémů.
NTLMv2	*(NT LAN Manager version 2)* autentizační protokol společnosti Microsoft používaný pro ověřování uživatelů v prostředí Windows.
NTP	*(Network Time Protocol)* je protokol pro synchronizaci času v počítačových sítích.
OSI	*(Open Systems Interconnection)* Referenční sedmivrstvý ISO/OSI model slouží pro standardizaci řešení a popisu počítačových sítí podle normy ISO 7498.
OSPF	*(Open Shortest Path First)* je směrovací protokol pro vnitřní sítě, který používá Dijkstrův algoritmus k nalezení nejkratší

	cesty. Podporuje hierarchické členění sítě do oblastí (areas) a rychle reaguje na změny topologie.
PE	*(Provider Edge)* Hraniční router MPLS sítě, na kterém jsou zakončeny VRF VPN nebo je prováděna manipulace s VRF VPN.
Radius	*(Remote Authentication Dial-In User Service)* protokol pro centrální ověřování a autorizaci uživatelů v síti.
Sandbox	Izolované testovací prostředí, kde lze bezpečně spouštět a analyzovat potenciálně nebezpečný kód nebo malware bez rizika ohrožení produkčních systémů.
SIEM	*(Security Information and Event Management)* Řešení zabezpečení, které organizacím pomáhá detekovat hrozby, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy/organizace.
SLA	*(Service Level Agreement)* je smluvně stanovená úroveň poskytovaných služeb mezi dodavatelem a odběratelem.
SFP	*(Small Form-factor Pluggable)* modulární síťové rozhraní.
SNMP	*(Simple Network Management Protocol)* protokol pro vzdálené monitorování a správu síťových zařízení.
SSO	*(Single Sign-On)* je metoda přihlašování umožňující přístup k více systémům po jediném ověření identity.
Syslog	Protokol pro sběr a přenos systémových a bezpečnostních logů ze zařízení do centrálního systému.
TLS	*(Transport Layer Security)* protokol pro šifrovanou komunikaci v počítačových sítích.
VLAN	*(Virtual Local Area Network)* je logické oddělení síťových segmentů na jedné fyzické infrastruktuře.
VoKB	Vyhláška 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.
VPN	*(Virtual Private Network)* Virtuální privátní síť – prostředek pro důvěryhodné propojení komponent informačního systému v rámci obecně nezabezpečené komunikační sítě. Při navazování spojení je obvykle vyžadována autentizace, komunikace je většinou šifrována.
VRF	*(Virtual Routing and Forwarding)* Virtuální směrování a předávání je technologie, která v počítačových sítích založených na protokolu IP umožňuje souběžnou existenci

	více instancí směrovací tabulky v rámci sítě stejného směrovače ve stejnou dobu.
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
ZTE	(ZTE Corporation) čínský výrobce technologií, uveden ve varování NÚKIB.

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace týkající se veřejné zakázky s názvem „Segmentace sítě " (dále jen „veřejná zakázka"), pro organizaci Správa železnic, státní organizace (dále jen „SŽ" nebo „Zadavatel"). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

2.1 Záměr SŽ v oblasti segmentace uživatelské sítě

SŽ, v roli správce kritické infrastruktury, ve věci požadavků opatření ve vazbě na vyhlášku o kybernetické bezpečnosti (VoKB), konkrétně § 18, je povinna zajistit, aby byl implementován systematický přístup k ochraně integrity svých sítí prostřednictvím segmentace a řízeného přístupu, čímž se minimalizuje riziko neoprávněného přístupu a šíření kybernetických hrozeb v rámci sítě.

Segmentace uživatelské sítě – stávající uživatelská síť, která je většinově založena na Cisco prvcích, není v současné době logicky segmentována a slouží pro účely všech zařízení, uživatelů, a to i pro aplikace třetích stran. Záměrem je vytvoření nových VRF sítí a provedení migrace menších logicky oddělených částí sítě do těchto VRF. Tento přístup posiluje kybernetickou bezpečnost organizace hned několika způsoby:

- **Izolace citlivých dat.** Segmentace umožňuje vytvořit bezpečnostní zóny podle důležitosti a citlivosti dat, která jsou v nich uložena. Takovéto rozdělení omezuje možnost neoprávněného nahlížení do citlivých informací a chrání před pokusy o jejich zneužití.
- **Prevence šíření útoků.** V případě úspěšného proniknutí do jednoho segmentu, zůstávají ostatní části sítě izolovány a chráněny díky předem definovaným přístupovým pravidlům mezi segmenty. To znamená, že útočník nemůže snadno přejít do dalších částí sítě a pokračovat v útoku. Segmentace tímto způsobem výrazně omezuje dopad bezpečnostního incidentu a zkracuje čas potřebný k reakci na útok.
- **Detailní správa přístupů a pravidel mezi jednotlivými segmenty sítě.** Segmentace umožňuje správci sítě vytvářet přesná pravidla řízení přístupu mezi jednotlivými částmi sítě podle role uživatelů a zařízení. Tím lze snadno uplatnit bezpečnostní princip minimálních oprávnění („least privilege"), který zajišťuje, že uživatelé mají přístup pouze k nezbytným částem sítě.

2.2 Předmět plnění veřejné zakázky

Předmětem plnění této veřejné zakázky je realizace zákonné povinnosti Zadavatele (dle § 18 VoKB), posílením odolnosti síťové infrastruktury proti kybernetickým hrozbám **dodávkou technologie Next-Generation Firewall** (dále jen NGFW) v návaznosti na segmentaci uživatelské sítě Zadavatele pro jednotlivá oblastní ředitelství, implementace a konfigurace dodané technologie,

odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Zadavatele.

Nedílnou součástí plnění jsou také vedle technické podpory dodaných technologií, pravidelné aktualizace bezpečnostních funkcionalit a post-implementační podpora Zadavatele i realizační a analytické práce při stanovování celkové koncepce „Segmentace sítě".

Očekávaným výstupem, kromě hardwarové dodávky požadovaného počtu firewallů a souvisejících komponent (viz. kapitola 3.2 tohoto dokumentu), je Dodavatelská participace na vytvoření koncepce segmentace uživatelské sítě, tj. kromě analytické části i zpracování detailního návrhu projektového implementačního postupu konfiguračních prací pro vybranou část sítě, která bude sloužit jako implementační vzor, který bude následně již Zadavatelem implementován do zbytku sítě vycházející ze specifikace uvedené v příloze č. 13.

Koncepce segmentace uživatelské sítě musí zohledňovat požadavky na snadnou správu a efektivní řešení případných bezpečnostních incidentů a ochranu před útoky, a to nejen z vnějšího prostředí, ale také v případě interních hrozeb.

Implementační postup vytvořený v rámci plnění této veřejné zakázky bude otestován na vybrané pilotní lokalitě v regionu Praha, technická specifikace pilotní lokality bude výstupem analytické části plnění této zakázky. Finální Implementační plán potom představuje souhrnný dokument, jehož cílem je definovat harmonogram a metodiku zavádění síťové segmentace do jednotlivých lokalit. Součástí Implementačního plánu je i podrobný implementační postup konfigurace síťových prvků, který popisuje konkrétní technické kroky nutné k dosažení cílového stavu, včetně návrhu síťových pravidel, topologie a přidělení adresních rozsahů.

3 Požadavky na plnění

Plnění veřejné zakázky se musí skládat z níže uvedených částí:

- Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ a návrh rozvoje sítě z pohledu její segmentace s pilotní realizací.
  - Zhodnocení stávající síťové infrastruktury SŽ.
  - Specifikace změn architektury segmentované uživatelské sítě (konfigurační práce při realizaci segmentace uživatelské sítě SŽ).
  - Analýza a návrh řešení pro specifikum geo-redundance.
  - Příprava implementačních kroků pro realizaci vlastní segmentace.
  - Implementační plán pro celou uživatelskou síť.
- Dodávka celkem 12 kusů NGFW a související komponentů dle uvedené specifikace.
  - Dodávka a implementace Next Generation Firewall.
  - Dodávka SFP+ modulů.
  - Dodávka licencí na provoz dodaných nástrojů.
  - Zajištění napojení nových NGFW do nástroje pro centrální správu NGFW.
- Odborné školení správy a údržby dodaných technologií.

- Post-implementační a technická podpora.
- Konzultační služby na vyžádání.

3.1 Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ a návrh rozvoje sítě z pohledu její segmentace s pilotní realizací

Cílem Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ, která je většinově založena na Cisco prvcích, je návrh rozvoje sítě z pohledu segmentace a vytvoření komplexního strategicko-funkčního dokumentu, který bude tvořen minimálně těmito částmi:

- Zhodnocení stávající síťové infrastruktury dle dodaných podkladů SŽ.
- Specifikace změn architektury segmentované uživatelské sítě.
- Návrh a verifikace zapojení NGFW se stávajícími routery.
- Analýza a návrh řešení pro specifikum geo-redundance.
- Příprava implementačních kroků pro realizaci vlastní segmentace v pilotní lokalitě v regionu Praha.
- Implementační plán pro celou uživatelskou síť.

Očekávaný informační rozsah jednotlivých oblastí, včetně definice odpovědností a činností Zadavatele a Dodavatele je uveden níže v jednotlivých podkapitolách.

Doplňující informace popisující technické prostředí Zadavatele a požadavky je blíže popsáno v příloze č. 12 a č. 13.

Zadavatel v rámci plnění této veřejné zakázky počítá s nastavením úzké spolupráce mezi týmy Zadavatele a Dodavatele, kdy Dodavatel bude vytvářet požadované výstupy definované tímto dokumentem a Zadavatel bude výstupy připomínkovat a na základě schválených výstupů realizovat konkrétní konfigurační kroky pro realizaci segmentace sítě.

3.1.1 Zhodnocení stávající síťové infrastruktury SŽ

Cílem první oblasti je zhodnotit stávající síťovou infrastrukturu uživatelské sítě Zadavatele. Pro potřeby tohoto zhodnocení poskytne Zadavatel Dodavateli níže uvedené podklady. Dodavatel na základě uvedených podkladů a případně dodatečně vyžádaných podkladů zpracuje finální výstup popisující současný stav a návrh budoucích kroků k realizaci požadované segmentace.

Vymezení rozsahu analýzy:

Cílem této fáze je zhodnocení stávající síťové infrastruktury uživatelské sítě Zadavatele a návrh budoucích kroků vedoucích k její segmentaci. S ohledem na povahu prostředí a dostupné kapacity je touto technickou specifikací upřesněn a vymezen rozsah analýzy.

Podklady dodané Zadavatelem budou sloužit jako primární vstup do analýzy. Je však třeba počítat s tím, že některé dokumenty budou vyžadovat doplnění v

průběhu analýzy. Poskytnutí všech informací nemusí být okamžité a některé detaily mohou být dostupné pouze v omezeném rozsahu.

Po celou dobu trvání analýzy Zadavatel určí pracovníka odpovědného za koordinaci součinnosti, který bude zastávat roli hlavního kontaktního bodu pro Dodavatele.

Tento pracovník bude podle potřeby zajišťovat komunikaci s dalšími odbornými rolemi Zadavatele (např. správci infrastruktury, bezpečnostní specialisté apod.).

Zadavatel neočekává detailní specifikace v následujících bodech:

- Podrobnou analýzu přístupové vrstvy sítě.
- Analýzu na úrovni L2, tedy jednotlivých přepínačů v lokalitách, fyzických rozhraní a jejich konfigurací (např. portových nastavení).
- Verifikaci všech síťových toků a závislostí mezi zařízeními na úrovni jednotlivých VLAN nebo portů.
- Komplexní analýzu konfigurací každého jednotlivého síťového prvku.

Současná kapacitní struktura uživatelské sítě jako je počet CE routerů je uvedena v příloze č.12 – Popis prostředí.

Účastník	Požadavek

Zadavatel	**Dodané podklady Zadavatelem**
	• Podklady síťové infrastruktury:
	  ○ Výstupy z ETS (CMDB).
	  ○ Výstupy z IP Fabric.
	  ○ Schémata topologie sítě.
	• Návrh koncepce segmentace uživatelské sítě SŽ.
	• Inventarizace síťových zařízení a jejich konfigurací.
	• Seznam současných síťových toků a závislostí.
	• Seznam aplikací a služeb třetích stran.
	• Návrh pilotní lokality v regionu Praha.

Dodavatel	**Výstup Dodavatele** • Zhodnocení návrhu koncepce segmentace uživatelské sítě SŽ (případné formování návrhů Dodavatele na modifikaci). • Zhodnocení zdrojů a kontrola souladu současného stavu s požadavky ZoKB a VoKB, případně NIS2 a dalšími platnými souvisejícími předpisy (dle platné legislativy), a GDPR a souvisejícími právními předpisy (identifikace konkrétních nesouladů).

- Analytický výstup popisující přístup řešení dále uvedených oblastí v prostředí SŽ (definování postupu kroků v rámci segmentace, specifikace postupu vlastní konfigurace, stanovení pořadí konfigurace jednotlivých prvků, přístup k migraci, definice rizik a jejich mitigace).
- Zhodnocení vstupů a konsolidace výkonnostních parametrů routerů, zdali jsou technologicky připraveny z hlediska nové VRF segmentace.
- Odsouhlasený návrh pilotu v požadované pilotní lokalitě.

3.1.2 Specifikace změn architektury

Předmětem této části je návrh změny architektury uživatelské sítě a definice pravidel segmentace ze strany Dodavatele, a to na základě podkladů od Zadavatele.
Výstupem bude návrhový dokument obsahující strukturu segmentace, bezpečnostní pravidla a technické detaily řešení dle níže uvedených požadavků.

Součástí dodávky bude vytvoření testovacích scénářů pro ověření funkčnosti nastavených pravidel. Verifikace bude provedena v rámci akceptace fáze Zadavatelem. Koncepce předpokládaného řešení je uvedena v příloze č. 13.

Oblast	**Činnost**
Základní specifikace změn architektury	**Výstup Dodavatele** • Schéma zapojení NGFW ve vrstvách L1 – L3 OSI modelu. • Definice segmentačních pravidel routování VRF • Popis komponent nové architektury. • Návrh změn propojení mezi PE a CE routery. Dokumentace bezpečnostních mechanismů pro NGFW.
Definice VRF instancí a jejich účelu	**Výstup Dodavatele** Analytický výstup Dodavatele musí pokrývat níže uvedené oblasti: • Seznam nových VRF instancí. • Popis účelu každé VRF instance. • Definice „routovacích" politik mezi VRF. • Návrh bezpečnostních politik pro každou VRF. • Definice IPv4 adresních rozsahů pro každý segment. • Rezervace adresních rozsahů pro budoucí růst. • Dokumentace překryvných sítí pro VRF.

	• Plán pro migraci IP adres.
Definice postupu konfiguračních prací	**Výstup Dodavatele** Analytický výstup Dodavatele musí pokrývat níže uvedené oblasti: • Návrh nastavení konfiguračních pravidel. • Pořadí konfigurace jednotlivých prvků. • Plán migrace do nových segmentů sítě. • Návrh implementace Koncepce segmentace SŽ. do prostředí pilotní lokality. • Návrh nastavení implementačních postupů. • Návrh procesního zajištění konfigurace v rámci organizace SŽ.

3.1.3 Analýza a návrh řešení pro specifikum geo-redundance

SŽ aktuálně disponuje dvěma konektivitami do sítě Internet, v Praze a Plzni.

Na základě úvodní části *3.1.1 Zhodnocení stávající síťové infrastruktury SŽ* a *3.1.2 Specifikace změn architektury* segmentované sítě dojde k vytvoření analytického výstupu pro možnosti nastavení geo-redundance konektivity v těchto lokalitách.

Analytický výstup musí pokrývat minimálně tato témata:

- Zhodnocení stávajícího stavu.
- Návrh infrastrukturního nastavení obou lokalit v režimu Active – Passive, příp. Active – Active.

3.1.4 Příprava implementačních kroků pro realizaci vlastní segmentace v pilotní lokalitě

Příprava implementačních kroků pro realizaci vlastní segmentace v závislosti na inventuře stávající sítě ve spolupráci s provozními složkami Zadavatele v pilotní lokalitě. Cílem této implementační části je provést segmentaci v rámci pilotního provozu vydefinované a schválené lokalitě takovým způsobem, aby pověření pracovníci Zadavatele mohli provádět segmentaci sítě v budoucnu již bez asistence ze strany Dodavatele.

Role Dodavatele v této fázi je podpůrná, konzultační, poskytuje doporučení. Vlastní konfigurační práce budou vykonávány pracovníky Zadavatele.

Oblast	**Činnost**
Příprava prostředí	Zajistí Zadavatel • Fyzická instalace NGFW do prostředí SŽ. Zajistí Dodavatel

	• Konfigurace NGFW v prostředí SŽ přes definované VPN připojení.
Nastavení VRF v prostředí SŽ	**Zajistí Zadavatel** • Vytvoření testovacích VRF instancí. • Konfigurační specifikace směrování mezi VRF. • Specifikace implementace bezpečnostních politik.
Implementace směrovacích protokolů – routing	**Zajistí Zadavatel** • Konfigurace BGP pro páteřní směrování. • Nastavení OSPF pro interní směrování. • Implementace redundantních cest. • Optimalizace směrovacích metrik. • Testování „failover" scénářů. • Vytvoření testovacích scénářů (podléhá odsouhlasením Zadavatele).
Testovací prostředí a zátěžové testy v síti SŽ, případně v testovacím prostředí Dodavatele	**Zajistí Zadavatel** • Definice typu testování • Testování maximální propustnosti. • Validace latence a jiter. • Stress testy bezpečnostních funkcí. • Testování vysoké dostupnosti (trhací testy). **Zajistí Dodavatel** • Příprava testovacích dat (konzultace). • Testy izolace mezi VRF (konzultace). • Poskytnutí testovacího prostředí (generátor provozu) pro testování NGFW pravidel definovaných během analýzy.
Bezpečnostní testování	**Zajistí Zadavatel** • Validace segmentace. • Testování bezpečnostních politik. • Ověření logování a auditních záznamů. • Návrh analýzy bezpečnostních rizik. **Zajistí Dodavatel** • Plnou podporu při identifikaci a odstranění nálezů z testování a návrh nápravných opatření. • Spolupráce na implementaci nápravných opatření.
Optimalizace konfigurace	**Zajistí Zadavatel** • Dokumentace provedených změn.

- Na základě zjištění Dodavatel uvede návrh optimalizace konfigurace.

3.1.5 Implementační plán pro celou uživatelskou síť

Na základě části *3.1.1 Zhodnocení stávající síťové infrastruktury SŽ* a *3.1.2 Specifikace změn architektury* segmentované sítě a úspěšně otestovaném pilotním řešení pro definovanou pilotní lokalitu, dle článku *3.1.4*, Dodavatel připraví detailní plán segmentace (jak postupovat) pro další lokality uživatelské sítě v prostředí SŽ.

Oblast	Činnost
Implementační plán	**Výstup Dodavatele** Na základě úspěšně otestovaného pilotního řešení vytvoření dokumentu, popisujícího kroky pro provedení segmentace pro další lokality v následujícím časovém období. Je očekáváno, že primární výstupem Dodavatele bude zpracování detailního návrhu projektového implementačního postupu konfiguračních prací. Výstup musí být aplikovatelný pro každou lokalitu (šest oblastních ředitelství) a musí minimálně obsahovat: • Časový harmonogram implementace. • Rozdělení úkolů a odpovědností mezi členy týmu SŽ. • Postup pro konfiguraci síťových zařízení (přepínače, směrovače, firewally). • Plán migrace existujících systémů do nových segmentů.
Rozvojový plán	**Výstup Dodavatele** Vytvoření dokumentu, který navrhne strategii s ohledem na budoucí další dílčí segmentaci v rámci pokračování projektu a budoucího rozvoje. • Nastavení postupů pro izolaci napadené části sítě • Nastavení pravidel pro detekci hrozeb • Optimalizace bezpečnostních nastavení

3.2 Dodávka celkem 12 kusů NGFW a souvisejících komponentů dle uvedené specifikace

3.2.1 Technické požadavky na dodávku Next Generation Firewall

3.2.1.1 Technická specifikace položky A:

V oblasti dodávky **dvou (2)** kusů zařízení NGFW definuje Zadavatel následující požadavky pro každé z nich:

Oblast	Požadavek
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
Minimální počet 25 Gbps rozhraní	4x SFP+
Minimální počet 10 Gbps rozhraní	4x SFP+
Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS a/nebo IDS, Aplikační kontrola	Minimálně 40 Gbps provozu označovaného jako „Enterprise Mix traffic ".
SSL/TLS inspekce až do propustnosti	Minimálně 20 Gbps
Celková minimální propustnost	60 Gbps
Minimální propustnost NGFW	60 Gbps

3.2.1.2 Technická specifikace položky B:

V oblasti dodávky **deseti (10)** kusů zařízení NGFW definuje Zadavatel následující požadavky pro každé z nich:

Oblast	Požadavek
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
Minimální počet 25 Gbps rozhraní	4x SFP+
Minimální počet 10 Gbps rozhraní	4x SFP+

Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS a/nebo IDS, Aplikační kontrola	Minimálně 20 Gbps provozu označovaného jako „Enterprise Mix traffic ".
SSL/TLS inspekce	Minimálně 8 Gbps
Minimální propustnost IPS a/nebo IDS	30 Gbps
Minimální propustnost NGFW	30 Gbps

3.2.1.3 Obecné požadavky pro položky A i B:

Oblast	Požadavek
Propustnost SSL/TLS inspekce	Minimálně TLS 1.2 a TLS 1.3.
Interní virtualizace	Požadována možnost potencionální virtualizace (minimálně 2 samostatných administrativně nezávislých virtuálních zařízení bez nutnosti pořízení dodatečné licence).
Podpora pravidel na základě identit uživatelů	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.
Způsoby ověřování uživatelů či napojení na autentizační systémy	Podpora proaktivního ověřování pomocí protokolu LDAP, NTLMv2, RADIUS a TACACS+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.
Módy vysoké dostupnosti klastru	Podpora režimů Active-Passive.
Aplikační kontrola	Detekce a řízení síťových aplikací. minimálně 4000 rozpoznávaných aplikací.
Směrování provozu	Podpora statického, policy based a dynamického směrování provozu.
Velikost lokálního úložiště	Minimálně 100 GB.
Ochrana proti DoS a DDoS útokům	Ano.

Podpora pravidel na základě identit uživatelů	Ano.
Vzdálená správa	• Vzdálená správa s dedikovaným vlastním portem 1Gbps. • Možnost vzdálené aktualizace firmware. • Podpora protokolu SNMP minimálně ve verzi 2c. • Podpora protokolu Syslog a předávání logů na vzdálený systém
Další funkcionality	Antibot, Ochrana DNS.
Podpora IPS a/nebo IDS	Licence by měla pokrývat funkcionality IPS a/nebo IDS v rozsahu funkčně obdobném se Snort 3 (reference snort.org) nebo lepším (licence pro inspekci HTTPS není podmínkou).
Napájení	2x napájecí zdroj AC 230 V.

Zařízení NGFW musí být dodány včetně veškerých potřebných licencí k provozu požadovaných služeb, viz. detailnější obecné požadavky uvedené v předchozí kapitole, s dobou platnosti a veškerými systémovými update po dobu 60 měsíců od ukončení fáze F2.1.

3.2.2 Dodávka SFP+ modulů

Požadujeme dodání kompatibilních SFP+ modulů pro dodaná NGFW zařízení v následujících počtech:

SFP+ Modul (Rychlost)	Počet
10 Gbps/25 Gbps	48 kusů.

Specifikace SFP+ modulů:

- Typ: Multimode.
- Konektor: LC duplex.
- Kompatibilita: NGFW zařízení dle specifikace výrobce
- Podpora rychlostí 10 Gbps i 25 Gbps
- DMI diagnostika.

3.2.3 Implementace Next Generation Firewall

V oblasti implementace NGFW pro jednotlivá OŘ jsou definovány následující činnosti, resp. požadavky:

Oblast	Činnost
Dodávka zařízení	Zadavatel požaduje dodávku zařízení do jedné lokality organizace SŽ v Praze. Tato lokalita bude upřesněna před ukončením fáze F1.1. Následná distribuce všech těchto zařízení do finálních lokalit a fyzická instalace do racků bude v režii Zadavatele.
Základní konfigurace	• Ověření zařízení na absenci HW vad. • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. ○ Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).
Konfigurace vysoké dostupnosti (HA)	Nasazení v režimu Active – Passive.
Síťová konfigurace	• Linková agregace. • IP adresace a VLAN tagy. • Směrování. • DHCP relay.
Vytvoření objektů a bezpečnostní politiky	• Specifikace nových pravidel pro nové NGFW. • Návrh jmenné konvence pravidel a objektů dle akceptované metodiky.
Dodavatel definuje vzorové bezpečnostní politiky dle vzoru Zadavatele	• IPS a/nebo IDS. • Application Control.
SSO Autentizace	Napojení na Active Directory řízení přístupů na základě identit.

3.2.4 Nástroj centrální správy NGFW

Zadavatel požaduje plnou kompatibilitu dodávaných firewallů s jedním ze současných nástrojů centrální správy a managementu, které již provozuje (Panorama a FMC – Firewall Management Center).

Pokud nebude možné zajistit plnou kompatibilitu dodávaných NGFW Dodavatelem se současným centrálním managementem, je Dodavatel povinen v rámci své dodávky dodat a naimplementovat v prostředí Zadavatele nový nástroj centrální

správy NGFW včetně příslušných licencí s dobou platnosti a veškerými systémovými update po dobu 60 měsíců od doručení nástroje centrální správy, který bude splňovat následující požadavky:

3.2.4.1 Požadavky na nástroj centrální správy NGFW

V oblasti dodávky nástroje pro centrální správu dodávaných NGFW definuje Zadavatel následující požadavky:

Oblast	Požadavek
Typ nástroje	Nástroj může být realizován jako fyzický nebo virtualizovaný, optimálně s podporou pro virtualizační platformu VMware.
Počet spravovaných zařízení	Nástroj centrální správy musí umožnit správu minimálně 12 fyzických zařízení.
Práce s událostmi	Nástroj centrální správy umožňuje příjem a uložení událostí v minimálním množství 10 GB událostí za den s možností licenčního rozšíření minimálně na 50 GB událostí za den.
Pokročilá analýza událostí	Nástroj centrální správy umožňuje základní analýzu událostí za účelem včasné identifikace reálné či potencionální hrozby. Primárně bude pro vyhodnocování incidentů používán nástroj aktuálně využívaný v prostředí SŽ, log management a SIEM.

V oblasti implementace nástroje centrální správy jsou Zadavatelem definovány následující činnosti, resp. požadavky:

Oblast	Činnost
Dodávka nástroje	Dodávka nástroje do lokality Praha. V případě virtualizovaného zařízení poskytnutí instalačních dat skrze internetovou konektivitu.
Základní konfigurace	• Ověření zařízení na absenci HW vad (pouze u fyzického zařízení). • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. ○ Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).

Připojení spravovaných zařízení	Integrace dodaných NGFW do centrální správy.
Součinnost při konfiguraci	Poskytnutí plné podpory Dodavatele při konfiguraci dodaného nástroje až po úplné spuštění nástroje pro centrální správu NGFW.

3.3 Školení

V oblasti odborného školení je požadováno následující plnění:

Typ školení	**Popis**
Základní školení	Úvodní seznámení s produktem pro 7 zástupců Zadavatele v rozsahu min. 1 MD a poskytnutí školících materiálů.
Odborné školení	Dodavatel zajistí pro 7 zástupců Zadavatele odpovídající, výrobcem NGFW certifikované, školení dodávané technologie, včetně nástroje centrální správy, které odpovídá požadavkům na každodenní správu a údržbu zařízení, správu z pohledu kybernetické bezpečnosti a kybernetického monitoringu (například představení kybernetických funkcionalit, jejich napojení na dohledové nástroje typu SIEM a využití NGFW pro forenzní šetření). Obecné požadavky na školení • Dodavatel poskytne Zadavateli kompletní školící materiály k dodávaným nástrojům. • Školení bude realizováno v rozsahu minimálně 3 MD. • Školení bude realizováno prezenční formou v lokalitě Praha. • Zadavatel bude moci pořídit z celého školení obrazový i zvukový záznam, který bude moci dále využívat pro potřeby školení vlastních pracovníků a externích partnerů. • Školení nemusí být zakončeno certifikační zkouškou.

3.4 Post-implementační a technická podpora

V oblasti post-implementační a technické podpory jsou definovány následující požadavky:

Oblast	Požadavky

Technická podpora výrobce	Zařízení nesmí mít oznámené EOS dříve než za 2 roky a oznámené EOL dříve než za 5 let. Dodavatel zajistí oficiální podporu výrobce po dobu 60 měsíců od dodávky technologií a licencí (fáze F2.1), která zahrnuje minimálně: • Režim podpory 8x5 (8 hodin denně v rámci pracovních dní, reakční doba 4 hodiny). • Doručení vadného dílu v režimu NBD. • Podpora dostupná na webovém portálu výrobce, e-mailu a telefonu. • Přístup k novým verzím firmware či OS. • Aktualizace bezpečnostních definic pro funkcionality definované v kapitole 3.1.
Post-implementační podpora Dodavatele	Dodavatel zajistí post-implementační podporu Zadavatele v rozsahu: (1) Poskytování expertních služeb, které budou využívány zejména pro podporu činností SŽ v případě řešení nestandardních stavů a pro profylaxi řešení, aby se předcházelo omezením jeho správné funkčnosti. (2) Konzultace při konfiguraci síťových komponentů a realizaci segmentační strategie definované výstupy této Veřejné zakázky. (3) Post-implementační podpora bude poskytována po dobu 5 let od ukončení fáze 4. (4) Post-implementační podpora bude poskytována v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy) podle servisního modelu A5). Plánované změny či významné změny (aktualizace, patch atd.) budou ze strany Dodavatele poskytnuty (uvolněny) SŽ vždy v pracovních dnech, a to konkrétně v pondělí a ve středu. V případě, že plánovaná změna či významná změna a její poskytnutí vychází na státní svátek, vyzve Dodavatel SŽ k upřesnění poskytnutí (uvolnění). (5) Poskytování služeb Helpdesku ze strany Dodavatele bude realizováno v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy) v Režimu 4 (5×8, tj. v pracovních dnech v době od 9:00 do 17:00 na telefonním čísle určeném Dodavatelem). (6) Měření SLA bude realizováno na straně Zadavatele.

odstranil: 3

odstranil: a bude poskytovat podporu na třetí úrovni (L3) v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy)

(7) Součinnost při auditech řešení, opravu a zapracování identifikovaných nedostatků.

3.5 Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

Oblast	Požadavky
Konfigurační konzultace a práce	Dodavatel poskytne konfigurační a konzultační práce prostřednictvím rolí **Seniorní systémový produktový inženýr, Specialista NGFW** v oblasti dodané technologie, který Zadavateli umožní konzultovat konfigurační parametry dodaného řešení.
Analytická konzultace	Dodavatel poskytne analytické konzultační práce prostřednictvím role **Systémový analytik** v oblasti dodané technologie, který Zadavateli umožní konzultovat analytické parametry dodaného řešení.

Maximální počet k čerpání všech Konzultačních služeb na vyžádání je 35 MD. Tyto služby budou čerpány až po akceptaci výstupů F1 a dodávky a implementaci komponentů F2. SŽ není povinna Konzultační služby na vyžádání čerpat.

4 Fáze dodávky a akceptační milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) je součástí jednoho z uvedených čtyř akceptačních milníků (A až D) a musí být Zadavatelem akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané akceptační fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky plnění.

Akceptační milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
A	F1.1	Zhodnocení stávající síťové infrastruktury	Akceptační protokol: • Zhodnocení návrhu koncepce segmentace uživatelské sítě SŽ • Zhodnocení souladu současného stavu s požadavky ZoKB, NIS2, GDPR, ISO IEC: 27033 v plném znění (identifikace konkrétních nesouladů) • Analytický výstup popisující přístup řešení v prostředí SŽ • Odsouhlasený návrh pilotu v požadované pilotní lokalitě	3.1.1
	F1.2	Základní školení	• Realizace školení s parafovanou prezenční listinou	3.3
B	F2.1	Dodávka NGFW a související komponentů dle uvedené specifikace	• Posouzení parametrů dodávaných komponent a Akceptační protokol: Dodávka NGFW dle specifikace ZD • Dodávka SFP+ modulů • Dodávka licencí dle funkční specifikace, viz. kapitola 3.2.1 • Dodávka nástroje centrální zprávy	3.2
C	F2.2	Specifikace změn architektury	Akceptační protokol: Pokrytí témat definovaných v bodu 3.1.2	3.1.2
D	F3.1	Implementace NGFW a související komponentů dle uvedené specifikace	Akceptační protokol: • Konfigurace komponent	3.2

Akceptační milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
			• Implementace NGFW do nástroje centrální správy	
D	F3.2	Příprava implementačních kroků pro realizaci vlastní segmentace	Akceptační protokol: • Pokrytí témat definovaných v bodu 3.1.4 • Na základě výstupu testování akceptace finálního návrhu	3.1.4
D	F4.1	Analýza a návrh řešení pro specifikum geo-redundance	Akceptační protokol potvrzující, že výstup obsahuje: • Zhodnocení stávajícího stavu • Návrh infrastrukturního nastavení obou lokalit v režimu Active - Active nebo Active - Passive	3.1.3
D	F4.2	Implementační plán pro celou uživatelskou síť SŽ	Akceptační protokol: • Zpracování detailního návrhu projektového implementačního postupu konfiguračních prací	3.1.5
	F4.3	Odborné školení	• Předání školících materiálů • Realizace školení • Realizace školení s parafovanou prezenční listinou	3.3
	F5	Post-implementační a technická podpora:	Fáze F5 bude vykazována na základě pravidelných měsíčních výkazů	3.4
	F6	Konzultační služby na vyžádání	Fáze F6 bude realizována na základě objednaných služeb dle příslušných objednávek	3.5

5 Vyloučení technologií

Vyloučení technologií představujících kybernetickou hrozbu

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: „Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:

***1.1.** Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*

***1.2.** ZTE Corporation, Šen-čen, Čínská lidová republika".*

Dne 4. ledna 2019 vydal Národní úřad pro kybernetickou a informační bezpečnost Metodiku k varování ze dne 17. prosince 2018 (dále jen „metodika"), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou Zadavatel provedl analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů. V návaznosti na to Zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

Zadavatel tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.