# Předběžná tržní konzultace ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem „*Segmentace sítě*“

# Příloha 1 - Rámcová specifikace předmětu plnění

## Záměr „Segmentace sítě“

Správa železnic (dále jako 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 představuje klíčový bezpečnostní prvek, jehož prostřednictvím dochází k logickému rozdělení síťové infrastruktury do oddělených celků. Toto řešení umožňuje efektivní řízení a monitoring síťového provozu mezi jednotlivými segmenty, čímž významně přispívá k celkové kybernetické bezpečnosti organizace.

Segmentace musí zohledňovat požadavky na snadnou správu a efektivní řešení případných bezpečnostních incidentů, kde patří mezi osvědčené strategie, které poskytují robustní ochranu před útoky, a to nejen z vnějšího prostředí, ale také v případě interních hrozeb.

**Záměr realizace zakázky spočívá v následujících bodech:**

**Segmentace uživatelské sítě,** rozdělení hlavní sítě na menší, logicky oddělené části, takzvané segmenty. 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.


Správa železniční dopravní cesty, 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.szdc.cz

**Správa železniční telematiky**
**V Celnici 1028/10**
**110 00 Praha 1**

## Popis prostředí

SŽ disponuje velmi rozsáhlým síťovým prostředím složeným z několika sítí. Jedná se o soubor technologických sítí zajišťujících kontrolu a provoz železniční dopravní cesty a uživatelské sítě poskytující konektivitu zaměstnancům a smluvním partnerům se systémy, které nemají přímý vliv na řízení železnice.

Celá oblast České republiky je propojena MPLS sítí, která přináší konektivitu se zbytkem sítě do jednotlivých regionů ČR. Jednotlivé lokality mají buď přímou konektivitu do MPLS sítě, nebo mají konektivitu zprostředkovanou přes jinou blízkou lokalitu. Propojení mezi těmito lokalitami je dále realizované pomocí protokolu IPv4.

Česká republika je rozdělena do několika oblastí (oblastní ředitelství SŽ (OŘ)), kde v každé oblasti fungují samostatné technologické sítě. Tyto sítě jsou od sebe odděleny na 3. vrstvě ISO/OSI modelu pomoci technologie VRF. Jednotlivé oblasti pak mají mezi sebou dále vytvořenou konektivitu pro vzájemné sdílení dat. Dále je přes celou ČR provozována uživatelská síť (UAS), předmět plnění, sloužící většině uživatelů a jiným než řídícím systémům. V rámci specifikovaných bodů v ČR (každý pro jednu nezávislou oblast, nadto i datová centra) jsou vytvořeny prostupy mezi technologickými síťemi a uživatelskou sítí.

Samotná segmentace proběhne díky VRF (Virtual Routing and Forwarding), která umožní logické oddělení různých částí sítě. Rozdělení reflektuje jak bezpečnostní požadavky, tak i praktické potřeby organizace. Každý segment bude mít jednoznačně definovaná pravidla pro komunikaci s ostatními segmenty, což významně zvýší celkovou bezpečnost sítě. Zároveň každé oblastní ředitelství bude vybaveno dvojicí nově implementovaných firewallů, do kterých bude sveden provoz celého oblastního ředitelství pro zvýšení úrovně provozního zabezpečení s možností detailní inspekce provozu v aplikační rovině, které budou zapojeny v HA režimu.

Vzhledem k historii rozvoje společnosti Správa železnic, je na její síť napojena řada třetích společností. Například na nádražích poskytují doplňkové služby, které nejsou součástí poskytovaných služeb Správy železnic. Jedním ze stěžejní požadavků je zmapování těchto služeb, potažmo aplikací a vyčlenění do vlastního adresního prostoru, pokud to bude možné, nebo úplně odstranit z uživatelské sítě.

## Specifikace požadavků

- Dodávka 12 kusů firewallů dle uvedené specifikace (příloha 2) spolu s požadovanými licencemi a nástrojem pro centrální správu
- Analýza stávající síťové infrastruktury uživatelské sítě
- Specifikace změn architektury segmentované uživatelské sítě
- Příprava implementačních kroků pro realizaci vlastní segmentace
- Nasazení technických prostředků realizace
- Zavedení monitorovacích a kontrolních mechanismů
- Specifikace budoucího rozvoje architektury
- Mapování aplikací a služeb třetích stran
- Analýza a návrh řešení pro specifikum geo-redundance

Očekávaným výstupem, kromě hardwarové dodávky 12 kusů firewalů a nástroje pro centrální správu, je pak vytvoření koncepce segmentace uživatelské sítě, tj. kromě analytické části i zpracování detailního návrhu projektového implementačního postupu konfiguračních prací pro vybranou část sítě, která potom bude sloužit jako implementační vzor s těmito parametry:

- Jak se bude postupovat?
- Jaké budou jednotlivé implementační kroky?
- Jak proběhne vlastní konfigurace?
- Jaké bude pořadí konfigurace jednotlivých prvků?

Tento implementační postup bude v rámci projektu otestován na vybrané a specifikované pilotní lokalitě v rámci úvodních kroků počáteční analýzy.

# Očekávaný harmonogram plnění

Očekáváme, že start projektu začne v 3. kvartálu 2025 s finálním milníkem realizace 31.7.2026 s těmito fázemi:

**Analytická část (1.10.2025 – 31.12.2025)**

1. Dokumentace stávající síťové infrastruktury
2. Inventarizace síťových zařízení a jejich konfigurací
3. Mapování současných síťových toků a závislostí
4. Mapování aplikací a služeb třetích stran
5. Popis stávajícího prostředí

Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.

**Specifikace změn architektury (1.1.2026 -31.3.2026)**

1. Základní specifikace
2. Definice VRF instancí a jejich účelu
3. Definice postupu konfiguračních prací

Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.

**Implementace / Realizace (1.4.2026 – 31.7.2026)**

1. Příprava prostředí
2. Nastavení VRF v testovacím prostředí
3. Implementace směrovacích protokolů
4. Příprava operačních procedur
5. Zátěžové testy
6. Bezpečnostní testování
7. Optimalizace konfigurace
8. Školení na nové technologie
9. Dodávka požadovaného HW

Klíčový výstup dodavatele: Aktivní kroky na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě naplňující následující úkoly:

1. Školení pracovníku SŽ
2. Nákup (doručení) 12 kusů NGFW dle dodané specifikace
3. Nastavení pilotní lokality, otestována a potvrzena funkčnost navrhovaného řešení
4. Zátěžové – bezpečnostní testování
5. Zapojení 12 NGWF v síti, nakonfigurování pravidel v rámci pilotní lokality
6. Optimalizace konfigurace
7. Rollout plán pro celou uživatelskou síť (akceptace zadavatelem)