

**Klasifikace: Diskrétní dokument**



Příloha č. 13 zadávací dokumentace

**Koncepce cílového stavu**

## Obsah

|     |                              |   |
|-----|------------------------------|---|
| 1   | Seznam zkratek .....         | 3 |
| 2   | Úvod .....                   | 4 |
| 3   | Požadavky .....              | 4 |
| 3.1 | VRF .....                    | 4 |
| 3.2 | Segmentační firewallly ..... | 5 |

## 1 Seznam zkratek

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

| Zkratka | Popis  |
|---------|--|
| HA      | ( <i>High Availability</i> ) je vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku.  |
| OŘ      | ( <i>Oblastní ředitelství</i> ) správní celek regionálního členění   |
| SŽ      | Správa železnic, státní organizace.  |
| UAS     | Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“.   |
| VRF     | ( <i>Virtual Routing and Forwarding</i> ) 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. |

## 2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace k veřejné zakázce s názvem „Segmentace sítě“. Dokument popisuje požadavky na segmentaci uživatelsko-aplikační sítě (UAS) ze strany organizace Správy železnic, státní organizace (dále jen SŽ), které jsou relevantní k poskytnutí účastníkům zadávacího řízení.

## 3 Požadavky

Implementace segmentace UAS bude vyžadovat pečlivé plánování a koordinaci, zejména vzhledem k rozsahu sítě a počtu dotčených systémů. Důležité bude zachování funkčnosti kritických služeb během celého procesu implementace.

### 3.1 VRF

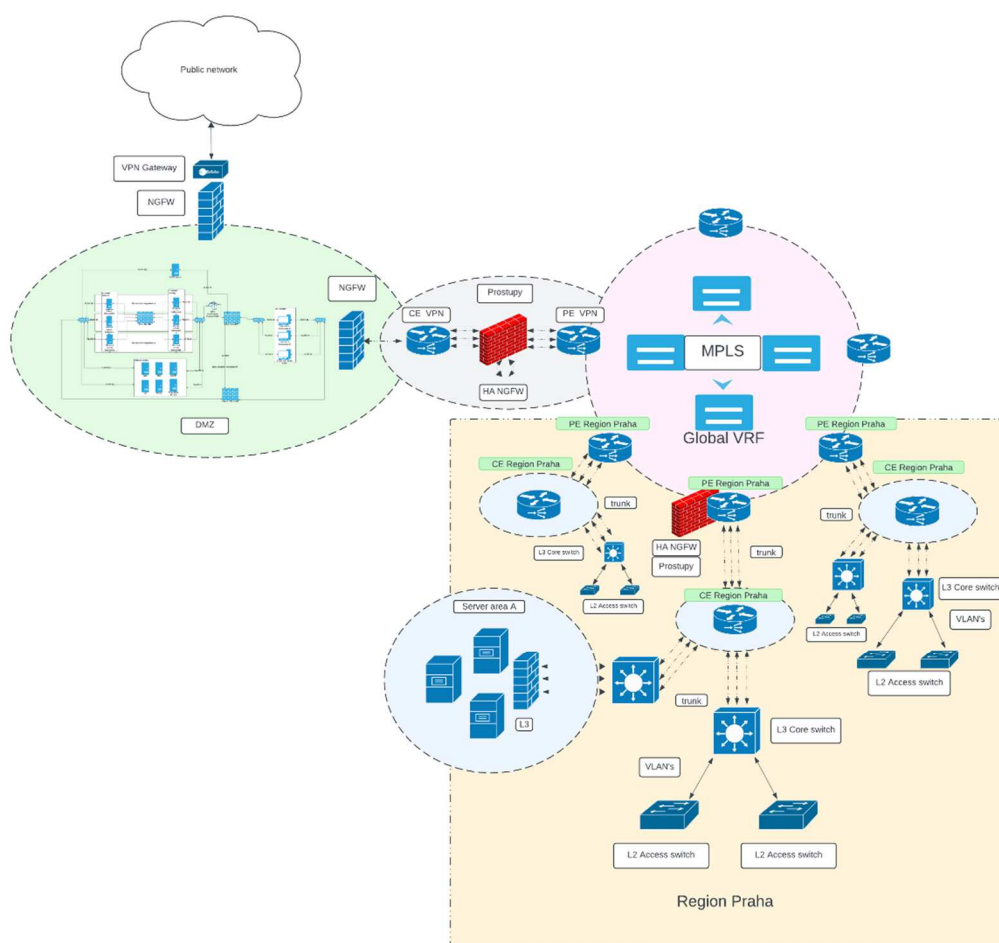
Samotná segmentace proběhne díky technologii VRF (Virtual Routing and Forwarding), která umožní logické oddělení různých částí sítě. Rozdělení reflektuje jak bezpečnostní požadavky, tak i praktické potřeby organizace vycházející z požadavků zákona o kybernetické bezpečnosti v návaznosti na níže popsané skupiny VRF. 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. Nové firewally budou zapojeny v HA režimu.

V současné době je celá uživatelská síť sjednocena v jedné VRF s názvem `szdc_global`. Předpoklad ze strany Zadavatele je vytvoření nových VRF popsaných v následující tabulce.

| Číslo | VRF                                 | Popis                                    |
|-------|-------------------------------------|--|
| 1     | Global ( <code>szdc_global</code> ) | Současná, již vytvořená VRF              |
| 2     | Users                               | Všechny uživatelské zařízení, zejména PC |
| 3     | Printers                            | Tiskárny, tiskové servery                |
| 4     | Network monitoring                  | Monitoring síťových prvků                |
| 5     | Server monitoring                   | Monitoring serverů                       |
| 6     | Guest                               | Striktně oddělená síť pro hosty          |
| 7     | IoT                                 | Media, dotykové panely, videokonference  |
| 8     | Servery                             | Serverová komunikace                     |
| 9 - x |                                     | Případné další VRF                       |

### 3.2 Segmentační firewally

Každé oblastní ředitelství (ORŽ) 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. Dvojice budou zapojeny v HA režimu.



Obrázek 1 – Předpokládaný způsob zapojení nových segmentačních firewallů