

NÁZEV AKCE: Segmentace provozu v technologické datové síti

PŘEDMĚT JEDNÁNÍ: Projednání připomínek

DATUM: 28. dubna 2021

MÍSTO: SUDOP PRAHA a.s., Olšanská 1a, Praha

ÚČASTNÍCI: Dle prezenční listiny

ZAZNAMENAL(A): Zpracovatelé PS a SO

Jednání bylo svoláno zhotovitelem projektové dokumentace ve spolupráci s investorem stavby, Stavební správou západ. Cílem jednání bylo projednat jednotlivé připomínky organizačních složek Správy železnic. a ostatních organizací k projektové dokumentaci stavby. Záznam z připomínkového jednání je proveden formou reakcí (odpovědí) k jednotlivým připomínkám a jejich zpracování je uvedeno v příloze tohoto záznamu.



Obsah

Správa železnic, Odbor příprav staveb (O6)	3
Správa železnic, Odbor zabezpečovací a telekom. techniky (O14)	4
Správa železnic, Odbor bezpečnosti a krizového řízení (O30)	11



Správa železnic, Odbor příprav staveb (06)

Zpracoval: Ing. Linková; 722 951 594; linkovaV@spravazeleznic.cz

1. Segmentace provozu v technologické datové síti:

- Opravte název investora.

Nelze opravit. Formulář má přednastavenou hodnotu, kterou nelze měnit (formulář je pod heslem). (Ing. Štrof)

- V listu 2A by měly být fakturace za náklady na Soutěže a zadávací řízení na projektovou přípravu (A.5.2.2.) a Soutěže a zadávací řízení na zhotovení stavby (A.5.2.3) provedeny před zahájením realizace (v roce 2021).

Bylo opraveno. (Ing. Štrof)

- Náklady za publicitu stavby (A.5.3.3) by měly být fakturovány v průběhu celé realizace.

Bylo opraveno. (Ing. Štrof)



Správa železnic, Odbor zabezpečovací a telekom. techniky (O14)

Zpracoval: Ing. Hora; 972 244 626; horav@spravazeleznice.cz

Připomínky O14 a CTD UŽT k DUR akce „Segmentace provozu v technologické datové síti“

Obecné technické připomínky

- V TDS není použitelné automatické řízení přístupu na základě IPS systémů, proto neuvažujeme o využití IPS licencí a není potřeba je nakupovat. Toto nemá vliv na použití IDS systémů a reportingu

Bylo opraveno a sjednoceno s připomínkou CTD. (Ing. Štrof).

- Projekt „Segmentace provozu v TDS“ *neřeší* provoz VSS kamer v síti SŽ a proto požadujeme výslovně uvést, že všechny kamery zmiňované v tomto projektu jsou kamery pro řízení provozu

V rámci zvolených VRF jsou VSS kamery vyčleněny do samostatné VRF (viz VRF - Kamery v budovách (mimo technologické prostory), Kamery na přejezdech) viz. kapitola 5.1. (Ing. Štrof)

- Tento projekt vůbec *neřeší* propusty mezi TDS a UAS, které jsou ale jednou z největších potenciálních zranitelností současné technologické datové sítě. Vzhledem k tomu, že projekt má za úkol posilovat kybernetickou bezpečnost sítě, požadujeme začlenění propustů a jejich technické řešení do tohoto nebo navazujících projektů.

Nutno definovat SŽ. Upřesnění nastavení politik a kontroly propustů mezi TDS a UAS. (Ing. Štrof)

- Předimplementační analýza a centrální části - stejně jako samotná konfigurace bude z větší části v pravomoci SŽ CTD a je proto na zvážení zahrnutí těchto činností do rozpočtu a nutno zpracovat technologický postup a časový harmonogram, neboť nebude v silách CTD nasazení ve všech lokalitách a OŘ v jednom termínu.

V rámci stavby je PS, ve kterém bude prováděna podrobnější analýza provozu, časový harmonogram nasazení segmentace apod. Náklady na činnosti prováděné SŽ CTD jsou právě v tomto PS zahrnuty. (Ing. Štrof)

Připomínky Ing. Tomáš Kříž, tel: 9722 44537, e-mail: krizt@spravazeleznice.cz

Dokument D_01_02_01_001

Kapitola 4.1

Měla by být popsána funkcionality FW: AVC, IDS, AMP.

Do textové části byly doplněny významy zkratk. (Ing. Štrof)

„Tyto firewally budou mít za úkol kontrolovat a sledovat provoz jak v rámci oblasti, tak i mezi nimi a provádět řízení politiky v souladu s vnitřními předpisy Správy železnic.“



(mezi oblastmi v rámci VRF nevidím důvod, alespoň v 1. Fázi segmentace) – nechceme filtrovat provoz v globálních VRF

Bylo opraveno. (Ing. Štrof)

Provoz změnit za provoz. Nepožadujeme kontrolovat a sledovat provoz mezi oblastmi.

Bylo opraveno. (Ing. Štrof)

Kapitola 4.3.1 Úrovně segmentace

Slovní spojení „virtuální síť LAN/VLAN“ není vhodné, protože znamená, virtuální síť lokální oblastní síť/virtuální lokální síť. Požadujeme přeformulovat v celém dokumentu.

Bylo opraveno. (Ing. Štrof)

IPS a IDS nepovažujeme za nástroj segmentace a požadujeme vynechat z textu.

Bylo opraveno a sjednoceno s připomínkou CTD. (Ing. Štrof)

Kapitola 4.3.2 Úrovně segmentace

„...ale rovněž i ochranu samotných komunikačních prvků (ACL, firewall systémy, IDS/IPS systémy atd.)“

Požadujeme popsat komunikační prvek ACL.

Bylo upraveno. Access list na síťových prvcích. Jedná se o způsob ochrany prvků a jedním z nich z nich je ACL. (Ing. Štrof)

Kapitola 5 Návrh technického řešení

„Další úrovní je hierarchická segmentace, kdy provoz z jednotlivých OŘ přechází do příslušného segmentu páteřní (globální) sítě. Tento princip tak umožňuje minimalizaci L2 segmentů, optimalizaci L3 segmentů a zajišťuje možnost kontroly a řízení provozu mezi jednotlivými segmenty. Z hlediska správy dovolí segmentace při vhodné implementaci řídit provoz v síti na základě relativně malých segmentů, které tak v případě bezpečnostního nebo provozního incidentu nebudou nevhodně ovlivňovat provoz v ostatních segmentech.“

Požadujeme vysvětlit pojmy: hierarchická segmentace a princip minimalizace L2 segmentů. Dále požadujeme upravit znění celého odstavce do srozumitelné formy.

V TZ je pod tímto pojmem myšlena globální hierarchie vs. hierarchie OŘ. (Ing. Štrof)

5.1 Segmenty

„Kontrola provozu bude prováděna vždy na hranicích mezi jednotlivými segmenty viz dále“

Nepožadujeme takováto pravidla pro definování segmentu a nechceme v rámci VRF řízení a kontrolu toků mezi OŘ pomocí FW. Nechceme filtrovat provoz v globálních VRF.



Bylo opraveno. (Ing. Štrof)

Kapitola 5.3 Architektura segmentace

„Firewally budou pracovat v L3 režimu a zadavatel může rozhodnout o jejich provozování v HA režimu.“

FW budou v L3 režimu, ale mezi CE routery jednotlivých VRF budou pracovat na L2. L3 routery budou tvořeny L3 switchi, které budou zároveň plnit funkci netflow sondy. Samotné FW se nepodílí na globálním routingu.

Jedná se záležitost konfigurace FW (L2/L3). Navržené zařízení umožňuje obě konfigurace zmíněné režimy neovlivňují volbu zařízení. (Ing. Štrof)

Požadujeme provoz v HA režimu, bez georedundance.

Bylo opraveno. (Ing. Štrof)

FW jsou zapojeny do PE routerů a ne do switchů. Požadujeme zapojení firewallů do CE switchů v souladu s filozofií MPLS provozu v síti SŽ, případně požadujeme vysvětlení proč má být pro FW vyhrazen PE router..

„...FW bude realizováno 10G spoji. Propojení bude realizováno prostřednictvím optických SFP modulů. Zadavatel požaduje zahrnout jako součást řešení i variantu, kdy pro každou lokalitu s FW bude na straně zadavatele v OŘ vyčleněný stávající samostatný PE router dedikovaný pouze pro provoz FW.“

Bylo doplněno. Technické řešení je zvoleno ve variantách, které nemají vliv na investiční náklady. Tzn., že FW mohou být připojeny do PE i CE.

Kapitola 5.4 Řízení prostupů na FW

„Firewall v OŘ kontroluje komunikaci:

mezi různými VRF v daném OŘ

z určité VRF v OŘ do globálního VRF stejného určení. Tzn. např. z VRF VOICE v OŘ do globální VRF VOICE.“

Firewall nefiltruje provoz mezi VRF stejného určení v různých OŘ.

Bylo opraveno. (Ing. Štrof)



Kapitola 5.14 PS 3-108 Před implementační analýza a centrální části

„Bude provedena technologická a topologická segmentace prezentována v kapitolách výše. Po provedení segmentace provozu v TDS se očekává v rámci přenosové sítě Správy železnic minimalizace L2 segmentů, větší bezpečnost, kontrola provozu, omezení šíření chyb, minimalizace broadcast domén a zvýšení robustnosti bezpečnosti v rámci OR.“

Co znamená pojem minimalizace L2 segmentů? Požadujeme vysvětlit.

Minimalizace L2 segmentů znamená omezení broadcast domén. Navrhuje se držet L2 segmenty co nejmenší, rozsahu a přenos řešit primárně přes L3. (Ing. Štrof)

Požadujeme začlenit O14 + CTD UŽT do zadání a vyhodnocení implementační analýzy.

Bylo doplněno. (Ing. Štrof)

Dokument D_01_02_02_001

PE z OR jsou zapojeny jen do Brna a Plzně a ne také do Prahy a Přerova.

Bylo opraveno. (Ing. Štrof)

Požadujeme dodat skutečné propojení do 4 P routerů a sladit polohopis lokalit s názvy objektů. Opravit popisy v obrázcích např. konflikt Plzeň x Praha hl.n.

Bylo opraveno. (Ing. Štrof)

Přípomínky Ing. Arnošt Dudek, tel. 972 244 485, e-mail: dudek@spravazeleznic.cz

Dokument D_01_02_01_001

Kap. 2.1

Opravdu nemá SŽ definovanou bezpečnostní politiku VRF/VPN sítí? S touto formulací bych nakládal velice opatrně. Je nutné vyčlenit ze stávající sítě nejen externí subjekty, ale i systémy KII. Doporučujeme upravit text.

Bylo opraveno. (Ing. Štrof)

Kap. 4.2

Doporučujeme doplnit konkrétní lokality i pro případnou georedundanci. Ve většině míst přichází v úvahu větší počet lokalit, které je nutno v DUR přesně specifikovat. Nutno rozhodnout, která varianta bude zvolena, v DUR by nemělo být uváděno variantní řešení. Chybějící podklady: pro a proti jednotlivých variant.

Geograficky oddělená lokalita byla jednou z variant. Po jednání s O14 a CTD je řešena pouze varianta v HA provedení v rámci OR. (Ing. Štrof).



Kap. 4.3.2

Doporučujeme redukovat požadavky uvedené v odrážkách na str. 7 na ty, které mají být součástí této stavby. Součástí pravděpodobně nebude např. akvizice, vývoj a údržba KII a významných informačních systémů atd.

Bylo opraveno. (Ing. Štrof)

Kap. 5.2

Nutno upřesnit pojem geograficky oddělená lokalita. Ve větších městech si lze pod geograficky oddělenou lokalitou představit např. různé čtvrti.

Geograficky oddělená lokalita byla jednou z variant. Po jednání s O14 a CTD je řešena pouze varianta v HA provedení v rámci OŘ. (Ing. Štrof).

Kap. 5.4

Doporučujeme doplnit, jak budou řešeny prostupy do/z jednotlivých VRF/VPN z Intranetu/Internetu.

Bylo doplněno. Bude řešeno samostatně VRF. Definice politik se nakonfiguruje na úrovni OŘ. (Ing. Štrof)

Doporučujeme doplnit, jak budou řešeny prostupy v rámci jednotlivých VRF/VPN, např. z různých VPN (ACL v jednotlivých VRF/VPN?).

Bylo doplněno. (Ing. Štrof)

Doporučujeme doplnit, kdo a jak definuje pravidla pro jednotlivé FW při uvádění do provozu. Bude defaultní stav vše zakázáno nebo vše povoleno?

Pravidla pro FW musí určit zadavatel právě před uváděním do provozu. Musí být součástí dalšího stupně dokumentace. (Ing. Štrof)

Připomínky Ing. Vladimír Hora, tel. 724630015, e-mail: horav@spravazeleznic.cz

Dokument D_01_02_01_001

Kap. 5.13 Dokument umísťuje technologie do lokality Ostrava – Svinov, kde je technologická místnost plně obsazena a plánuje se přesun technologií do uzlu Ostrava – Vítkovice. Požadujeme zohlednění této eventuality a koordinaci těchto akcí. Totéž platí pro umísťování technologií do žst Brno – Maloměřice, kde se plánuje přesun do žst. Brno – Židenice.

Jedná se o dodávku FW v HA provedení, které lze do navržených lokalit umístit a ve kterých je v současné době dostatečná konektivita i napájení. (Ing. Štrof)



Kap. 5.14 Tento projekt bude klást vysoké nároky na koordinaci i jednotlivých prací a bude obsahovat značné množství konfigurační práce ze strany CTD. Proto požadujeme do prováděcího projektu rozpracovat detailní časový harmonogram prací na jednotlivých OŘ centra.

Projektant s připomínkou souhlasí. Předpokládá se, že v dalším stupni bude proveden detailnější rozbor prací i jeho harmonogram. Je popsáno v TZ. (Ing. Štrof)

Připomínky Ing. Raimund Moliš, tel: 972 741 210, e-mail: molis@spravazeleznic.cz

Dokument D_01_02_01_001

Kapitola 4.3.1.1

Přístup z Intranetu bude muset být, Včetně VPN veden přes JUMP servery, které budou asi součástí stavby O30.

Bylo doplněno. (Ing. Štrof)

Kapitola 5.3

Firewally budou v HA řešení v jedné lokalitě s IDS a budou připojeny na CE L3switch.

Bylo opraveno a sjednoceno s připomínkou O14. Připojení FW je řešeno variantně bez vlivu na investiční náklady. (Ing. Štrof)

Firewall bude řídit komunikaci mezi VRF pro danou OŘ (stažená komunikace z MPLS v daném OŘ) včetně přístupů z intranetu.

Bylo opraveno. (Ing. Štrof)

Kapitola 5.1

CCTV - firewall bude řídit pouze přístup pro VRF dopravních kamer, provoz kamer VSS musí být zajištěn jiným způsobem.

Firewall nebude řídit provoz v rámci jedné VRF mezi jednotlivými OŘ.

Dle segmentace jsou dopravní kamery v samostatné VRF mimo FW. (Ing. Štrof)

Provoz mezi různými VRF mezi OŘ bude jako doposud řešit skupina globálních Firewallů na CDP Praha a Přerov.

Bylo opraveno. (Ing. Štrof)

Konfigurace je ověřována v lokalitě OŘ Plzeň a je nutno dodat, že zahrnuje konfiguraci všech MPLS v daném OŘ.

Bylo doplněno. (Ing. Štrof)



Kapitola 5.6

Doplnit licence, záruky a podporu na 60 měsíců.

Záruka na zařízení dle TKP je 60 měsíců. Délka podpory a licencí je 24 měsíců. (Ing. Štrof)



Správa železnic, Odbor bezpečnosti a krizového řízení (030)

Zpracoval: Ing. Knížek; 724 931 668; knizek@spravazeleznic.cz

Odbor bezpečnosti a krizového řízení prošel předloženou projektovou dokumentací stavby a sděluje:

1. Požární bezpečnost (Knížek)

V dokumentaci část **B. Souhrnná technická zpráva**, bylo zjištěno:

Zásadní připomínky:

a) **čl. B.6.1, písm. g) Závěrečné hodnocení**, jsou uvedeny neplatné dokumenty SŽ a proto se požaduje jejich oprava, např. takto:

stávající text vypustit:

„Při stavebních a montážních pracích je nutno dodržovat protipožární opatření v návaznosti na předpis SŽDC Ob 14 a Směrnici SŽDC č. 56.“

návrh nového textu:

„Při stavebních a montážních pracích je nutno dodržovat protipožární opatření v návaznosti na řád R14 - Řád zabezpečení požární ochrany státní organizace Správa železnic“.

Bylo opraveno. (Ing. Štrof)

Ostatní připomínky:

b) **čl. B.6.1, písm. g) Závěrečné hodnocení**, je uveden nepřesný název JPO a proto se navrhuje jeho oprava:

stávající nepřesný název:

„...JPO Hasičské záchranné služby...“

nově:

„...JPO Hasičského záchranného sboru Správy železnic...“ nebo *“...JPO HZS Správy železnic...”*

Bylo opraveno. (Ing. Štrof)

2. Objektová bezpečnost (Ing. Krylová), kybernetická bezpečnost (Kříž)

Bez připomínek.

