

Váš dopis zn. Systém C.E.Sta
Ze dne 17.3.2021
Naše zn. 25305/2021-SŽ-GŘ-O14
Listů/příloh 4/0

Vyřizuje Ing. Vladimír HORA
Telefon +420 972 244 626
Mobil +420 724 630 015
E-mail horav@spravazeleznic.cz

Datum 8. dubna 2021

pouze elektronicky:
Správa železnic, s.o.
Škarvadová Monika
Skarvadova@spravazeleznic.cz
Systém C.E.Sta

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.
- 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
- Tento projekt vůbec *neřeší* prostupy 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 postupů a jejich technické řešení do tohoto nebo navazujících projektů.
- 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.

Připomínky Ing. Tomáš Kríž, tel: 9722 44537, e-mail: krizt@spravazeleznic.cz

Dokument D_01_02_01_001

Kapitola 4.1

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

„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

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

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.

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

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.

Kapitola 5 Návrh technického řešení

„Další úroveň 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.

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.

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.

Požadujeme provoz v HA režimu, bez georedundance.

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.“

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.

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 OŘ.“

Co znamená pojem minimalizace L2 segmentů? Požadujeme vysvětlit.

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

Dokument D_01_02_02_001

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

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.

Připomínky 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.

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.

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.

Kap. 5.2

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

Kap. 5.4

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

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

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

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.

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.

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.

Kapitola 5.3

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

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

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.

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

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

Kapitola 5.6

Doplnit licence, záruky a podporu na 60 měsíců.

S pozdravem

Ing. Martin Krupička

ředitel odboru zabezpečovací a
telekomunikační techniky