ZMĚNOVÝ POŽADAVEK
ZP019_GFŘ

NÁVRH NA ZMĚNU PROJEKTU (ZP)

Project ID	Projekt GFŘ
Objednatel	GFŘ
Krátký název ZP	**Úpravy síťové infrastruktury pro projekt IDR – rozvojové činnosti**
Datum podání	12.03.2021
Datum aktualizace ZP	
Priorita	Střední
Předkladatel	GFŘ, [redacted] vedoucí Projektu za Objednatele
Zhotovitel	SPCSS, [redacted] manažer služeb za Poskytovatele

1. ZADÁNÍ

1.1 Shrnutí zadání

Předmětem zadání změnového požadavku jsou rozvojové činnosti, které se týkají úpravy síťové infrastruktury pro projekt IDR a provedení zátěžového testu infrastruktury. Tyto jsou poskytovány formou služby (dále jen „Služba").

1.1 Zadání požadované změny

Příprava a realizace úpravy síťové infrastruktury pro projekt IDR na sdílené infrastruktuře SPCSS pro GFŘ včetně provedení zátěžových testů.

1.1.1 Popis požadované změny

1. Příprava a vyjasnění rozsahu a požadavků na prostředí IDR
2. Analýza dopadu změn na sdílenou infrastrukturu, zejména FW, F5 a síťové prostředí ADIS v SPCSS
3. Vypracování designu změn
4. Realizace změn v prostředí SPCSS/ADIS pro všechna požadovaná prostředí
5. Testování a ladění prostředí s GFŘ, IBM a O2 ITS
6. Předání a akceptace projektu

Samostatně je realizován zátěžový test infrastruktury ADIS – zajištění testu síťové infrastruktury a WAF F5 jako dílčí část testu pro oddělení provozu ADIS.

1.1.2 Dopady na stávající Službu

Změny propojení a rekonfigurace aktivních prvků v souladu s požadavky Objednatele.

1.1.3 Specifikace SW a HW požadavků

Nejsou definovány žádné HW a SW požadavky.

1.2 Popis zajištění realizace změny

Zajištění změn a realizace na požadavek Objednatele dodavatelem ANECT.

1.3 Zdůvodnění změny

Požadavek Objednatele na úprava infrastruktury v rámci projektu PMD/IDR.

VÝSLEDEK	☒ Dále zpracovávat ☐ Nerealizovat ☐ Přepracovat ☐ Odložit

	Schválil (SPCSS)	**Schválil (GFŘ)**
Jméno	[redacted] manažer služeb za SPCSS	[redacted] vedoucí Projektu za GFŘ
Datum dle elektronického podpisu	6. 4. 2021	6. 4. 2021
Podpis		

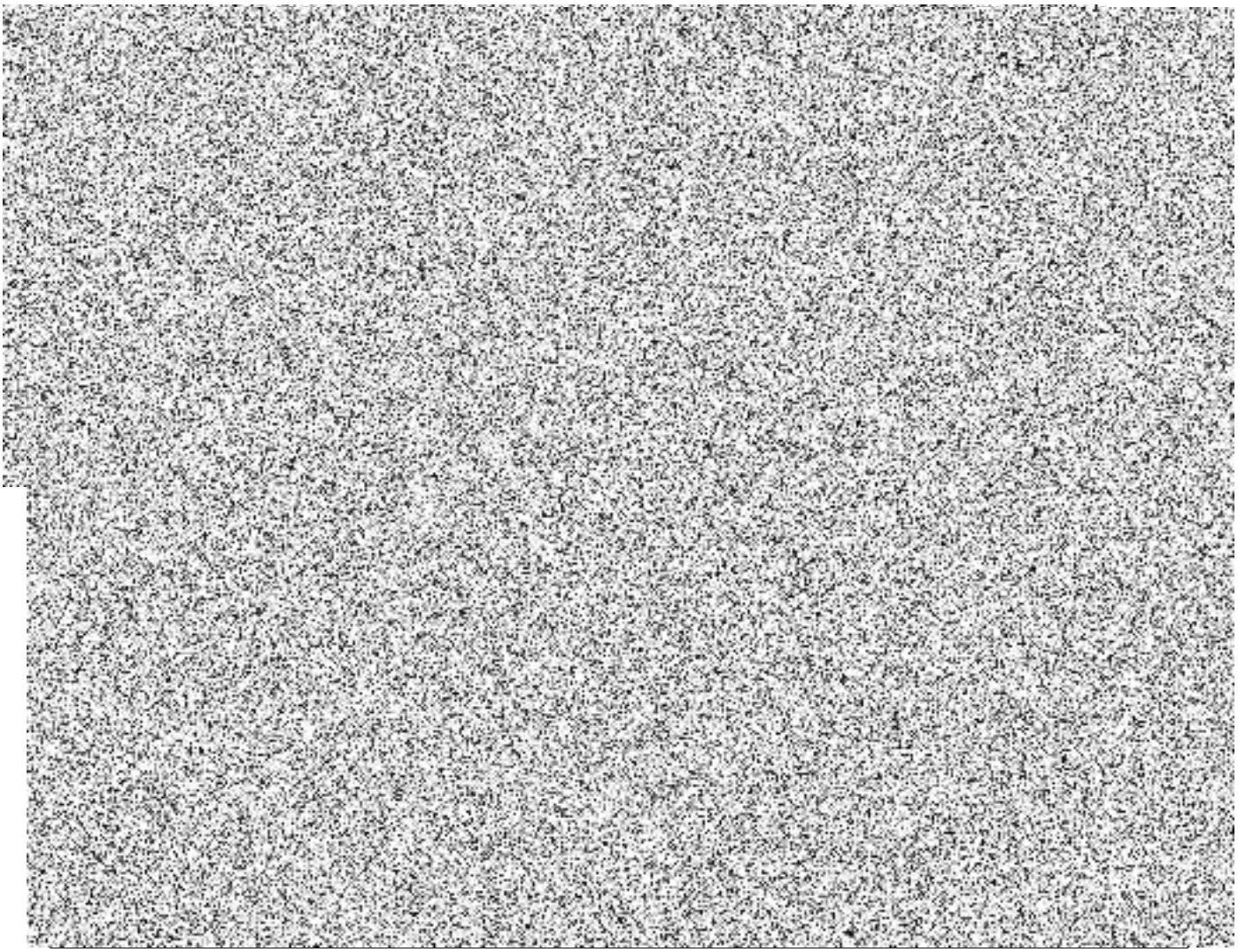
2. ANALÝZA ZP – TECHNICKÉ ŘEŠENÍ

1.2 Detailní popis řešení

Účelem je popsat změny v konfiguraci prostředí stávajícího Daňového portálu, které bude nutno aplikovat na balanceru F5 a síťové infrastruktuře v závislosti na vyžadovaných změnách aplikačního a komunikačního prostředí pro nasazení IDR.
Požadované změny infrastruktury zasahují jednak do prvků spravovaných SPCSS, ale vlastněných GFR (Nexus switche a F5). Jednak také do prvků sdílené infrastrukrury BDP pro ADIS (FW GFŘ v SPCSS).
Součinnost musí být vykonána s dodavateli aplikace ADIS/PMD (IBM) a jednotlivými odděleními ADIS a infrastruktury GFR (ADIS provoz - K. Kubát, Infrastruktura - L. Novotný, Bezpečnost - OBI, Achitekti a rozvoj – J. Bohm).

2.1.1 Popis současného stavu

Stávající řešení pro ADIS využívá síťové prvky Nexus 5548UP včetně Fabric Extenderů pro rozšíření portové kapacity, loadbalancery F5, webové proxy a část infrastruktury SPCSS (internetové switche a virtuální firewally). Infrastruktura stávajícího stavu je zobrazena na následujícím obrázku.



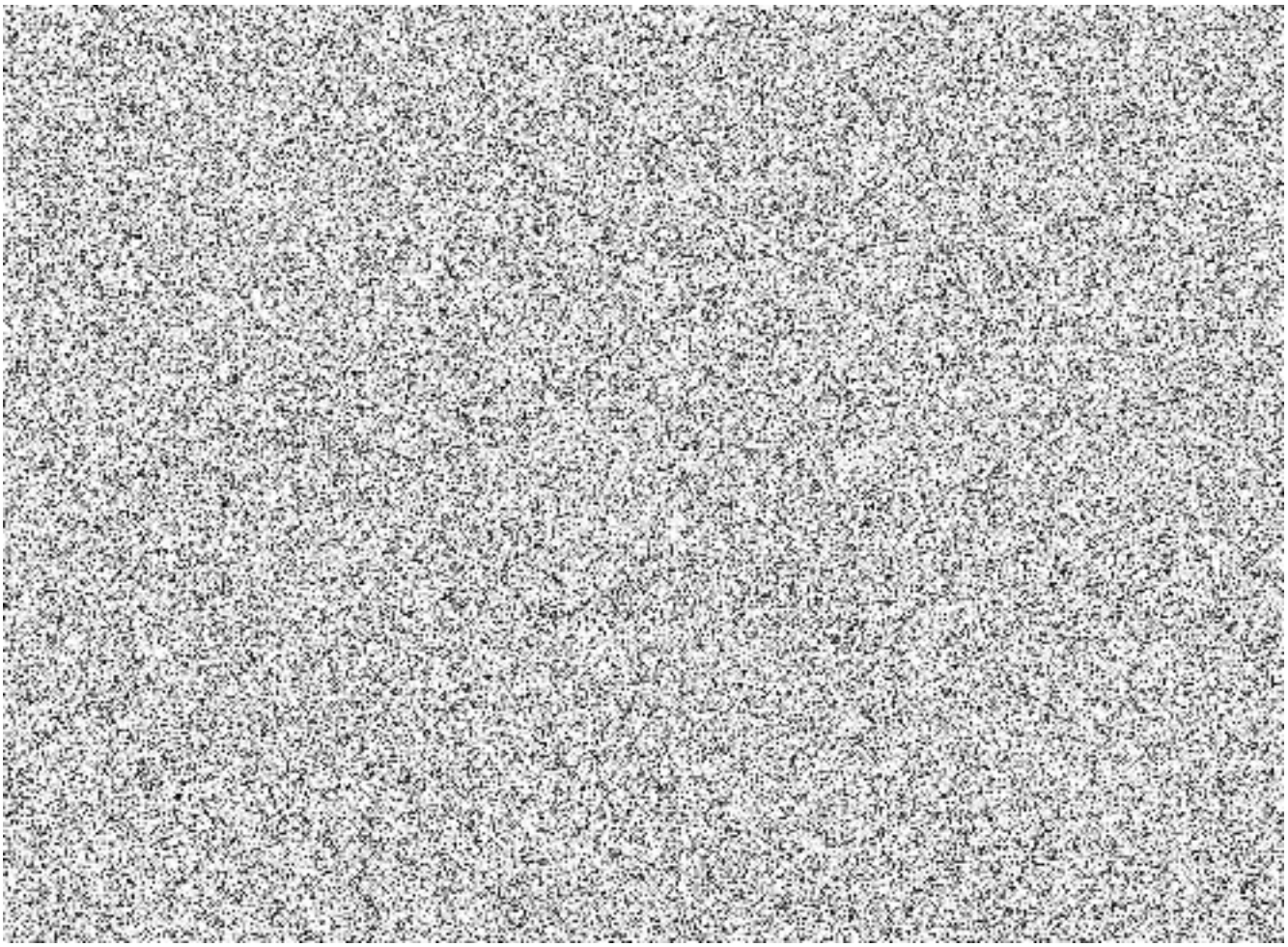
1.2.1 Cílový stav

Infrastruktura cílového stavu bude síťově oddělena od stávající infrastruktury ADIS. Fyzicky bude využívat stejné síťové prostředky, oddělení bude na úrovni VLAN a virtuálních směrovacích instancí. Prostupy mezi prostředími budou řízeny bezpečnostními pravidly. Backendové komunikace a management provoz interní infrastruktury bude řízen access-listy na přepínačích. Produkční provoz a management provoz externí infrastruktury bude terminován na virtuálním stavovém firewallu a řízen pravidly tohoto firewallu. Terminace TLS a rozkládání zátěže bude řešeno na dedikované virtuální instanci loadbalanceru F5.

Komunikace z IDR na služby zveřejněné do Centrálního místa služeb (CMS) bude probíhat přes stávající proxy servery GFŘ pro ADIS. Zveřejnění služeb IDR do CMS bude napřímo přes loadbalancery F5.

V rámci infrastruktury budou existovat 2 prostředí – produkční a testovací, které budou od sebe vzájemně odděleny s využitím VLAN. Komunikace bude řízena bezpečnostními pravidly.

Infrastruktura cílového stavu je zobrazena na následujícím obrázku.



Rozpis jednotlivých činností.

A. Konfigurace síťového prostředí

Vzhledem k požadavku na virtuální oddělení nové infrastruktury od stávajících sítí pro ADIS je potřeba nakonfigurovat na přepínačích nové VLAN včetně jejich nastavení na propoje (trunky) a na přístupové porty.

Obecně platí, že VLANy budou roztažené přes obě datová centra, což umožní migraci virtuálních serverů mezi DC. Subnety budou zpravidla velikosti /24, kdy v každém DC budou zařízení adresována z jedné poloviny subnetu. V každém DC bude vlastní výchozí brána. Zařízení využívají vždy výchozí bránu v datovém centru, kde budou fyzicky připojena, jinak bude docházet k suboptimálnímu asymetrickému směrování odchozího a návratového provozu. Při migraci virtuálních serverů mezi DC musí dojít i k rekonfiguraci IP rozhraní a výchozí brány.
Management VLAN budou terminovány na L3 přepínačích Nexus, kde budou i výchozí brány pro příslušný subnet včetně redundance výchozí brány protokolem HSRP. V rámci redundance budou existovat 2 HSRP skupiny, jedna bude aktivní v DC1 se zálohou v DC2 a druhá opačně.
Produkční VLAN budou zakončeny na loadbalancerových clusterech a budou přístupné pouze přes virtuální firewall GFR. Princip výchozích bran je obdobný k management VLAN, v každém DC bude vlastní výchozí brána.

Následující tabulky uvádí plánované fyzické zapojení a adresní plán.

Tabulka 2-1: Fyzické připojení serverů

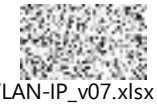
Switch	Port	Režim	Vlan
dc1eth1	Eth111/1/15	802.1Q trunk	1460-1467
	Eth112/1/15	802.1Q trunk	1460-1467
	Eth113/1/3	802.1Q trunk	1460-1463
dc1eth2	Eth111/1/15	802.1Q trunk	1460-1467
	Eth112/1/15	802.1Q trunk	1460-1467
	Eth113/1/3	802.1Q trunk	1460-1463
dc2eth1	Eth111/1/15	802.1Q trunk	1460-1467
	Eth112/1/15	802.1Q trunk	1460-1467
dc2eth2	Eth111/1/15	802.1Q trunk	1460-1467
	Eth112/1/15	802.1Q trunk	1460-1467

Tabulka 2-2: Adresní plán

VLAN name	VLAN ID	Subnet
IDR-MGM-EXT	1460	10.92.104.0/24
IDR-MGM-INT	1461	10.92.105.0/24
IDR-APP-INT	1462	10.92.106.0/24
IDR-APP-EXT	1463	10.92.107.0/24
IDR-MGM-EXT-T	1464	10.92.108.0/24
IDR-MGM-INT-T	1465	10.92.109.0/24
IDR-APP-INT-T	1466	10.92.110.0/24
IDR-APP-EXT-T	1467	10.92.111.0/24
GFR_DC1_IDR_DMZ	1468	10.92.112.0/27
GFR_DC2_IDR_DMZ	1469	10.92.112.32/27

GFR_DC1_IDR-INT_spoj1	1470	10.92.112.64/28
GFR_DC1_IDR-INT_spoj2	1471	10.92.112.80/28
GFR_DC2_IDR-INT_spoj1	1472	10.92.112.96/28
GFR_DC2_IDR-INT_spoj2	1473	10.92.112.112/28
GFR_IDR-EXT_FW_SPOJ	1474	10.92.112.128/28
GFR_IDR-EXT_SPOJ_N7K	1475	10.92.112.144/30
GFR_DC1_IDR-EXT_spoj1	1476	10.92.112.160/28
GFR_DC1_IDR-EXT_spoj2	1477	10.92.112.176/28
GFR_DC2_IDR-EXT_spoj1	1478	10.92.112.192/28
GFR_DC2_IDR-EXT_spoj2	1479	10.92.112.208/28

Tabulka 2-3: Kompletní adresace



VLAN-IP_v07.xlsx

B. Nastavení bezpečnostních pravidel

Externí (public facing) sítě budou terminované na stavovém virtuálním firewallu GFR kvůli vyšší bezpečnosti, interní sítě budou zabezpečeny bezstavovými ACL na přepínačích. Nastavení bezpečnostních pravidel je uvedeno v následujících vložených tabulkách.

Tabulka 2-4: Prostupy na stávající DataPower

Prostupy_IDR_Data Power.xlsx

Tabulka 2-5: Interní a externí prostupy

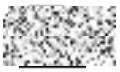
Prostupy_IDR_v4.xls x

C. Publikace služeb do CMS

Pro účely zveřejnění služeb do CMS (komunikace s eGON service bus) je třeba terminovat zabezpečené TLS spojení na loadbalancerech, kde bude zároveň rozkládána zátěž mezi aplikační servery. Detailní nastavení je uvedeno ve vložené tabulce níže.

1) Konfigurace loadbalancingu včetně testování dostupnosti aplikačních serverů.
2) Nasazení serverových certifikátů CA SZR testovacího i produkčního prostředí na F5. Dojde k ukončení TLS na F5
3) Nasazení privátních serverových certifikátů pro zabezpečení komunikace na aplikační servery.
4) Vkládání klientského certifikátu do HTTP hlavičky X-Client-Cert.

Tabulka 2-6: Nastavení loadbalancingu a terminace TLS.



LB-IDR_v03.xlsx

1.2.2 Realizované činnosti

ID	Činnost	Zodpovědnost
1.	Změny sdílené infrastruktury, kontext GFŘ	SPCSS

1.2.3 Požadovaná součinnost

1. Dohoda a koordinace při testování, přípravě releasu a nasazení s odd. provozu ADIS (p. Kubát)
2. Dohoda a koordinace s třetími stranami (O2, IBM)

2.2 Dopady do kvalitativních parametrů poskytované Služby

Bez dopadů

2.3 Harmonogram realizace

Realizace – od 05/2021 do 6/2021

2.4 Rizika

1. Součinnost SZR – generování certifikátů
2. Součinnost MVČR / Nakit – konfigurace služeb CMS
3. Součinnost GFŘ – žádost o služby CMS a certifikáty SZR.

2.5 Cenové ohodnocení pracnosti a nákladů (pokud budou nad rámec Služby)

Celková cena	V Kč bez DPH
Příprava - hrazena jednorázově	563 905,00
Měsíční cena	0,00

2.6 Dopady do dokumentací

ID	Název	Popis změny
1.	Provozní dokumentace	aktualizace dokumentu

3. SPOLEČNÁ SEKCE

Rozhodnutí

Datum	
Výsledek rozhodnutí	☒ Realizovat ☐ Nerealizovat ☐ Přepracovat ☐ Odložit
Podepsaná aktualizace smlouvy?	☐ Ano ☐ Ne ☒ Není potřeba

Podpisem oprávněné osoby potvrzujeme, že s návrhem změny výše popsané dle výsledku rozhodnutí souhlasíme. V případě výsledku Realizovat, je možné ihned zahájit práce na implementaci ZP.

V Praze dne dle elektronického podpisu:

Objednatel	**Zhotovitel**
Jméno: [redacted] **1. 6. 2021** Podpis: _____	Jméno: [redacted] 2. 6. 2021 Podpis: _____
Jméno: [redacted] **1. 6. 2021** Podpis: _____	Jméno: [redacted] **31. 5. 2021** Podpis: _____