# Příloha č. 1 Popis stávajícího hardwarového řešení

Obsah

## 1 Rekapitulace řešení

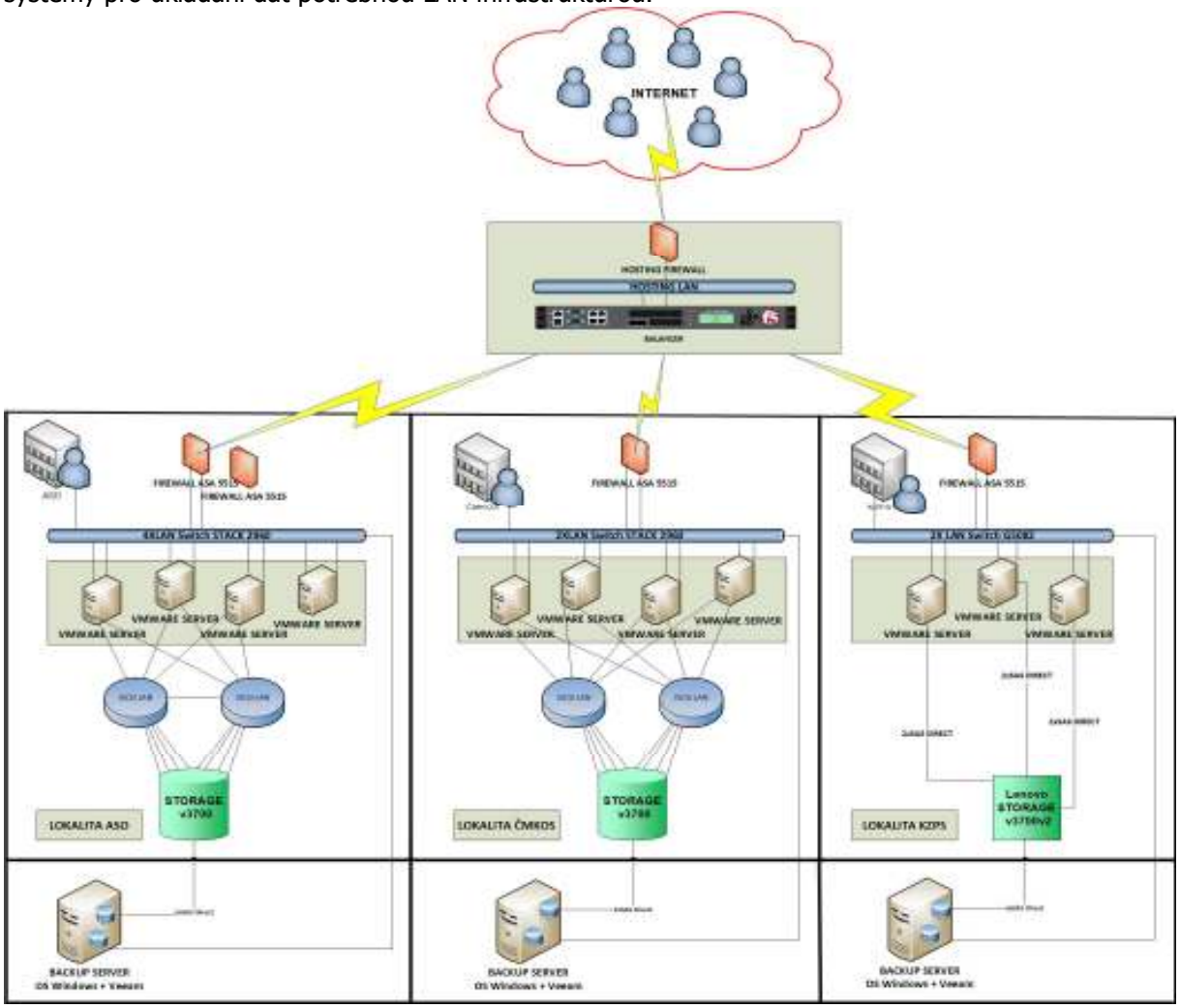
Pro řešení infrastruktury na provoz systémů aplikační vrstvy ASO iPodpora bylo realizováno řešení, které podporuje požadované zadání jak z pohledu fyzického rozmístění infrastruktury, tak i z pohledu počtů požadovaného hardware. Infrastruktura je distribuována mezi lokality, ASO/KZPS-CMKOS-Hostingové centrum.

Řešení je realizováno s rozmístěním aplikačního provozu, do tří oddělených uzlů. Lokality zadavatel-partner mají vytvořeny existující veřejné internetové propojení. V lokalitě zadavatel je umístěna infrastruktura pro ASO a KZPS, na lokalitě partnera pak infrastruktura CMKOS. V hostingovém centru je umístěn balancer, který rozděluje a zabezpečuje provoz v případě nedostupnosti primární lokality, kterou je infrastruktura ASO a automaticky směruje provoz aplikace z ostatních dostupných lokalit. Řešení je realizováno primárně jako virtualizované s vrstvou systému VMware vSphere. Provozní data jsou „replikována" mez lokalitami na úrovni databázové a aplikační vrstvy s využitím databázových nástrojů. V rámci tohoto řešení jsou použity prvky pro síťovou komunikaci a firewally pro zabezpečení a oddělení jednotlivých uzlů od lokální sítě LAN. Každá lokalita má oddělené zálohovací řešení se samostatným serverem a zálohovacím software.

Všechny výpočetní uzly jsou řešeny s plnou dualitou serverových, LAN, iSCSI a SAS komponentů. Na všech fyzických serverech je implementována virtualizační vrstva. V rámci virtualizační vrstvy jsou provozovány systémy VMware vSphere 5.5 a 6.5 Data jsou ukládána odděleně na disková pole. V uzlech ASO a CMKOS to je na disková pole připojená k serverům přes ethernetovou konektivitu a protokol iSCSI, uzel KZPS je realizován přes rozhraní SAS.

## 2 Architektura řešení

Architektura je blokově znázorněna na následujícím obrázku. Lokality jsou osazeny servery, storage systémy pro ukládání dat potřebnou LAN infrastrukturou.



# 3 Podrobný seznam dodaných komponent

## 3.1 Pro lokalitu ASO

| Part No. | Popis | Počet |
|---|---|---|
| 5458F2G | x3250 M5, Xeon 4C E3-1240v3 80W 3.4GHz/1600MHz/8MB, 1x8GB, O/Bay 2.5in HS SAS/SATA, SR H1110, 460W p/s, Rack | 4 |
| 00D5016 | 8GB (1x8GB, 2Rx8, 1.35V) PC3L-12800 CL11 ECC DDR3 1600MHz LP UDIMM | 12 |
| 90Y8877 | IBM 300GB 2.5in SFF G2HS 10K 6Gbps SAS HDD | 8 |
| 49Y4240 | Intel Ethernet Quad Port Server Adapter I340-T4 for IBM System x | 4 |
| 94Y6236 | IBM 460W Redundant Power Supply Unit with 80+ certified | 4 |
| 90Y3901 | IBM Integrated Management Module Advanced Upgrade | 4 |
| 00EN491 | HDD no return for System x | 4 |

| Part No. | Popis | Počet |
|---|---|---|
| 2072S2C | IBM Storwize V3700 SFF Dual Control Enclosure | 1 |
| 00Y2503 | 600GB 2.5In 10K rpm 6Gb SAS HDD | 24 |
| 00L4584 | 1Gb iSCSI 4 Port Host Interface Card | 2 |

## 3.2 Pro lokalitu CMKOS

| Part No. | Popis | Počet |
|---|---|---|
| 5458F2G | x3250 M5, Xeon 4C E3-1240v3 80W 3.4GHz/1600MHz/8MB, 1x8GB, O/Bay 2.5in HS SAS/SATA, SR H1110, 460W p/s, Rack | 4 |
| 00D5016 | 8GB (1x8GB, 2Rx8, 1.35V) PC3L-12800 CL11 ECC DDR3 1600MHz LP UDIMM | 12 |
| 90Y8877 | IBM 300GB 2.5in SFF G2HS 10K 6Gbps SAS HDD | 8 |
| 49Y4240 | Intel Ethernet Quad Port Server Adapter I340-T4 for IBM System x | 4 |
| 94Y6236 | IBM 460W Redundant Power Supply Unit with 80+ certified | 4 |
| 90Y3901 | IBM Integrated Management Module Advanced Upgrade | 4 |
| 00EN491 | HDD no return for System x | 4 |

| Part No. | Popis | Počet |
|---|---|---|
| 2072S2C | IBM Storwize V3700 SFF Dual Control Enclosure | 1 |
| 00Y2503 | 600GB 2.5In 10K rpm 6Gb SAS HDD | 24 |
| 00L4584 | 1Gb iSCSI 4 Port Host Interface Card | 2 |

## 3.3 Komponenty LAN a WAN pro lokality ASO a CMKOS

| Katalogové číslo | Popis | Kusů |
|---|---|---|
| **HW/SW** | | |
| **ASA5515-K9** | ASA 5515-X with SW 6GE Data 1 GE Mgmt AC 3DES/AES | 3 |
| SF-ASA-X-9.1-K8 | ASA 9.1 Software image for ASA 5500-X Series5585-X & ASA-SM | 3 |
| CAB-ACE | AC Power Cord (Europe) C13 CEE 7 1.5M | 3 |
| ASA-VPN-CLNT-K9 | Cisco VPN Client Software (Windows Solaris Linux Mac) | 3 |
| ASA5500-ENCR-K9 | ASA 5500 Strong Encryption License (3DES/AES) | 3 |
| ASA-ANYCONN-CSD-K9 | ASA 5500 AnyConnect Client + Cisco Security Desktop Software | 3 |
| ASA5515-MB | ASA 5515 IPS Part Number with which PCB Serial is associated | 3 |
| L-ASA-AC-E-5515= | AnyConnect Essentials VPN License - ASA 5515-X (250 Users) | 3 |
| L-ASA-AC-M-5515= | AnyConnect Mobile - ASA 5515-X (req. Essentials or Premium) | 3 |

| | | |
|---|---|---|
| WS-C2960X-24TS-L | Catalyst 2960-X 24 GigE 4 x 1G SFP LAN Base | 4 |
| CAB-ACE | AC Power Cord (Europe) C13 CEE 7 1.5M | 4 |
| **C2960X-STACK** | Catalyst 2960-X FlexStack Plus Stacking Module | 4 |
| CAB-STK-E-0.5M | Cisco FlexStack 50cm stacking cable | 4 |
| PWR-CLP | Power Retainer Clip For Cisco 3560-C and 2960-C Compact Swit | 4 |
| **WS-C2960X-48TS-L** | Catalyst 2960-X 48 GigE 4 x 1G SFP LAN Base | 2 |
| CAB-ACE | AC Power Cord (Europe) C13 CEE 7 1.5M | 2 |
| C2960X-STACK | Catalyst 2960-X FlexStack Plus Stacking Module | 2 |
| CAB-STK-E-0.5M | Cisco FlexStack 50cm stacking cable | 2 |
| PWR-CLP | Power Retainer Clip For Cisco 3560-C and 2960-C Compact Swit | 2 |

## 3.4 Pro lokalitu KZPS

| **Počet KS** | **Popis** |
|---|---|
| 3 | Server : ThinkSystem SR570 |
| 3 | Intel Xeon Bronze 3104 6C 85W 1.7GHz Processor |
| 3 | ThinkSystem 8GB TruDDR4 2666 MHz (1Rx8 1.2V) RDIMM |
| 6 | ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM |
| 3 | ThinkSystem 1Gb 2-port RJ45 LOM |
| 3 | ThinkSystem XClarity Controller Standard to Enterprise Upgrade |
| 6 | 2.8m, 10A/100-250V, C13 to C14 Jumper Cord |
| 3 | ThinkSystem M.2 CV1 32GB SATA 6Gbps Non-Hot Swap SSD |
| 3 | Companion part for XClarity Controller Standard to Enterprise Upgrade in factory |
| 3 | ThinkSystem Broadcom NetXtreme PCIe 1Gb 4-Port RJ45 Ethernet Adapter |
| 3 | ThinkSystem 430-8e SAS/SATA 12Gb HBA |
| 3 | ThinkSystem Screw-in Slide Rail Kit with 1U CMA |
| 6 | ThinkSystem 550W(230V/115V) Platinum Hot-Swap Power Supply |
| 3 | ThinkSystem SR590/SR570 MB |

## 3.5 Komponenty LAN a WAN pro KZPS

| PN | Popis zboží | Množství [ks] |
|---|---|---|
| ASA5516-FPWR-K8 | ASA 5516-X with FirePOWER services, 8GE, AC, DES | 1 |
| CAB-ACE | AC Power Cord (Europe), C13, CEE 7, 1.5M | 1 |
| SF-ASA-K-9.8-K8 | Cisco ASA 9.8 Software image for ASA 5506/5508/5516 series | 1 |
| SF-ASA-FP6.2-K9 | Cisco FirePOWER Software v6.2 for ASA 5500-X | 1 |
| ASA5516-CTRL-LIC | Cisco ASA5516 Control License | 1 |
| ASA5516-SSD | ASA 5516-X SSD | 1 |
| ASA5500-ENCR-K8 | ASA 5500 Base Encryption Level (DES) | 1 |
| L-AC-PLS-LIC= | Cisco AnyConnect Plus Term License, Total Authorized Users | 25 |
| CON-SNT-ASA556F8 | SNTC-8X5XNBD ASA 5516-X with FirePOWER services, 8GE | 1 |
| 7159G52 | RackSwitch G8052 (Rear to Front) | 2 |
| 90Y9462 | Console Cable Kit Spare | 2 |
| 00D6185 | Adjustable 19" 4 Post Rail Kit | 2 |
| 39Y7937 | 1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable | 4 |
| 90Y9427 | 1m Passive DAC SFP+ Cable | 4 |

## 4 Zálohované zdroje napájení

Každý uzel řešení je napájen z nepřerušitelného zdroje napájení UPS v následující konfiguraci:
Zařízení typu UPS je konvertibilní RACK/Tower UPS s výkonem 3kVA, RT3kVA.

Jedná se o zařízení, které nabízí a zabezpečuje výkonovou ochranu s rozšířenou účinností a jednoduchým power managementem pro ochranu a zvýšenou dostupnost zařízení jako jsou servery, LAN prvky diskové pole a ostatní IT prostředky. UPS garantuje při plném zatížení 4 minuty provozu. UPS jsou vybaveny modulem pro vzdálenou správu a software na podporu bezpečného ukončení provozu pro běžné operační systémy a VMware.

| Part No. | Popis | Počet |
|---|---|---|
| 55943KX | RT3kVA 2U Rack or Tower UPS (200-240VAC) | 3 |

## 5 Zálohovací řešení

Pro řešení zálohování dat v jednotlivých uzlech je v každém realizován jeden samostatný server. Celkem se tedy jedná o tři samostatná řešení. Každý server je s lokálním diskovým úložištěm sestaveným ze dvou disků v poli R1 pro implementaci operačního systému a zálohovacího software. Současně je na tomto serveru disková kapacita pro vlastní zálohy v odděleném poli sestaveným z šesti vysokokapacitních disků v poli R5. Každý server je připojen do sítě LAN přes 4x1Gbit. Také je každý server připojen napřímo k diskovým polím přes SAS řadič z důvodů realizace toku záloh typu Direct SAN Access. Servery disponují duálními napájecími zdroji a komponenty pro přestavbu na provedení do skříně Rack a licencemi pro nezávislé vzdálené ovládání a KVM management.

Operačním systémem zálohovacího řešení je Windows 2016 v edici Standard. Na tento je implementován zálohovací software Veeam backup ve free verzi.

Jako serverový HW jsou použity Lenovo ThinkSystem ST550 v následující konfiguraci:

| Počet KS | Název položky |
|---|---|
| 1 | ThinkSystem ST550 3.5" Chassis with 8 bays |
| 1 | CPU Intel Xeon Bronze 3104 6C 85W 1.7GHz Processor |
| 2 | ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM |
| 1 | ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter |
| 2 | ThinkSystem 3.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD |
| 6 | ThinkSystem 3.5" 6TB 7.2K SATA 6Gb Hot Swap 512e HDD |
| 1 | ThinkSystem I350-T4 PCIe 1Gb 4-Port RJ45 Ethernet Adapter |
| 1 | ThinkSystem 430-8e SAS/SATA 12Gb HBA |
| 1 | ThinkSystem XClarity Controller Standard to Enterprise Upgrade |
| 1 | Tower to Rack Conversion Kit |
| 2 | ThinkSystem 750W(230/115V) Platinum Hot-Swap Power Supply |
| 2 | 2.8m, 10A/100-250V, C13 to C14 Jumper Cord |
| 1 | Windows Server 2016 Per 16 Cores W2016 Std 16C ML NoPreinstal |

## 6 Infrastruktura

Všechny dodávané HW komponenty, resp. serverová farma, diskové pole, SAN a LAN infrastruktura, jsou rozmístěny v prostorách budov v ulici Tyršova 6 a nám. W. Churchilla 2.

### 6.1 Servery

Realizovaná technická infrastruktura vychází z požadavků z výběrových řízení a požadavků pro aplikační software. Architektura technické infrastruktury je navržena tak, aby splňovala nároky vysoké bezpečnosti, dostupnosti a výkonu. Je koncipována tak, aby umožňovala efektivní vertikální i horizontální škálovatelnost technické infrastruktury v závislosti na měnících se potřebách vyplývajících zejména z postupného zpřesňování požadovaných parametrů či nárůstu zátěže.

Servery jsou kalkulovány s kapacitní rezervou a jsou schopny zabezpečit provoz systémů i v případě „ztráty" jednoho serveru v lokalitě.

### 6.2 Servery v lokalitě ASO

Všechny dodávané servery a komponenty pro tuto lokalitu jsou umístěny do skříně RACK s kapacitou 20U. Výjimkou je server pro zálohování, který je umístěn mimo skříň RACK. Servery zaberou ve skříni celkem 4U pozice. Všechny servery jsou vybaveny interním managementem nezávislým na běhu OS a umožňující vzdálené převzetí konzole.

### 6.3 Servery v lokalitě ČMKOS

Dodávané servery pro tuto lokalitu jsou umístěny do samostatné skříně RACK. Tyto servery disponují stejnými komponenty a parametry, jako ty pro již popisovanou lokalitu ASO.

### 6.4 Servery pro lokalitu KZPS

Tyto servery byly dodány v rámci rozšíření stávající infrastruktury v důsledku integrace nového partnera. Servery a ostatní komponenty jsou umístěny v prostorách lokality Tyršova. Instalovány jsou společně do rozebíratelné skříně RACK o velikosti 20U. Všechny servery jsou opět vybaveny interním nezávislým managementem s možností vzdáleného ovládání serverů.

## 7 Technický popis serverů

### 7.1 Servery ASO a CMKOS - IBM x3250M5

**Charakteristika:**

- 1 procesor Intel Xeon Quad-Core
- Kapacita paměti až 32 GB
- Až 12 TB interní diskové kapacity
- Integrovaný duální Gigabit Ethernet
- Optimalizován do racku (1U)

### 7.2 Servery KZPS – SR570

Jsou použity 3 kusy serverů Lenovo ThinkSystem SR570.

Každý server je osazen jedním CPU Intel Xeon Bronze 3104 6C 85W 1.7GHz a pamětí RAM s kapacitou 40GB. Pro připojení k síti LAN je vybaven 6ti 1Gbit porty realizovanými on-board a doplňující 4portovou

kartou. Pro připojení k diskovému poli byla zvolena technologie SAS, proto je v konfiguraci duální řadič ThinkSystem 430-8e SAS/SATA 12Gb HBA. Součástí serveru jsou duální napájecí zdroje, licence pro nezávislý management serveru včetně KVM funkcí. Pro bootování hypervisoru je zde řešení s ThinkSystem M.2 CV1 32GB SATA 6Gbps Non-Hot Swap SSD diskem.

# 8 Disková pole

Kapacita pro ukládání dat je řešena diskovými poli pro blokový přístup, propojených do SAN. V každé lokalitě je umístěno jedno diskové pole IBM v3700 resp Lenovo v3700v2. Storage jsou vybaveny technologiemi pro podporu virtualizace a je možné rozšíření pro zajištění sync/async replikací, dle potřeby.

## 8.1 Disková pole ASO a CMKOS

Zde jsou použita disková pole IBM Storwize V3700. Pro připojení hostů je použito rozhraní ISCSI a SAS.

## 8.2 Diskové pole KZPS

S ohledem na virtualizační řešení jsou provozní data centralizována na diskovém poli. Pro toto řešení je použito diskové pole pro blokový přístup Lenovo V3700V2. Jedná se o rebrandované pole IBM v5010.

Toto rozdělení je shodné pro všechny lokality

# 9 Infrastruktura LAN

## 9.1 LAN ASO/CMKOS

LAN infrastruktura je navrhována na komponentech firmy CISCO. V obou lokalitách ASO/ČMKOS je infrastruktura pro LAN přepínače zdvojena pro bez výpadkový provoz serverů. Navíc je v lokalitě ASO fyzicky oddělen IP provoz pro infrastrukturu iSCSI k diskovému poli. LAN prvky jsou stohovány. Podle potřeb řešení je provedena konfigurace vLAN a začlenění do stávající LAN infrastruktury.

## 9.2 LAN KZPS

LAN infrastruktura je navrhována na komponentech firmy Lenovo RackSwitch G8052.

Pro lokalitu KZPS navrhujeme dva kusy těchto 48 portových přepínačů L3 propojených do jednoho celku (stohu) pomocí pasivních DAC SFP+ kabelů. Tato konfigurace eliminuje fyzickou nedostupnost jednoho přepínače a zjišťuje dostupnost serverové infrastruktury na LAN i v případě popisované hardwarové poruchy. Podle potřeb řešení je provedena konfigurace vLAN, routingu a začlenění do stávající LAN infrastruktury.

# 10 Balancer

Pro požadavky řešení směrování v případě výpadku některé lokality, nebo uzlu na lokalitě je implementováno zařízení BIG-IP i2600 DNS z produkce firmy F5 Networks.

Jedná se o hardwarový prvek, který řeší automatizaci směrování uživatelů k aplikacím podle definovaných pravidel na dostupnost jednotlivých lokalit, tak aby nebylo nutné řešit směrování ručně přes DNS záznam (současný stav). Balancer je umístěn v hostingovém centru integrátora řešení, mimo lokality ASO/ČMKOS/KZPS.

## 11 LAN v lokalitě ASO

V lokalitě zadavatele jsou instalovány 4 kusy 24portových LAN přepínačů Cisco **WS-C2960X-24TS-L.** Dva jsou použity pro segmentaci provozu LAN infrastruktury fyzických a virtuálních serverů. Zbylé 2 kus pak propojí infrastrukturu serverů a diskového pole pro protokol iSCSI. Takovým řešením dosáhneme fyzického oddělení těchto světů a zvýšíme výkonnost a bezpečnost. Tento způsob uplatňujeme pouze v této lokalitě, protože zde předpokládáme nevyšší provoz. V následující tabulce jsou uvedeny IP adresy pro managment jednotlivých LAN komponentů

## 12 LAN v lokalitě ČMKOS

V této lokalitě je použito stejné řešení, jako již bylo popsáno v předchozím odstavce. Hlavním rozdílem je počet použitých LAN přepínačů. Zde jsou osazeny 2 kusy 48portových LAN přepínačů Cisco **WS-C2960X-48TS-L.** Oddělení LAN segmentů je realizováno za pomocí vLAN.

## 13 Lan KZPS

Pro tuto část infrastruktury je použito řešení se síťovými přepínači Lenovo. Jsou osazeny 2 kusy 48portových LAN přepínačů Lenovo G8052. Oddělení LAN segmentů je realizováno za pomocí vLAN.

## 14 Bezpečnost

Pro zabezpečení připojení do internetu jsou v lokalitě ASO dva firewally zapojené v redundantním režimu. V záložních lokalitách a uzlech ČMKOS a KZPS je konfigurován jeden firewall stejného provedení.

Cisco ASA firewally z řady 5515/6-X jsou konfigurovány pro firewallovací i VPN funkcionalitu na primární a sekundární lokalitě. Firewall řídí provoz z Internetu na jednotlivé frontend servery, které nabízejí aplikační služby do Internetu.

V primární lokalitě ASO josu Cisco ASA firewally instalovány ve dvojici v tzv. failoveru. V případě výpadku primárního zařízení dojde k přesunu veškerého provozu na záložní prvek. Tento provoz se zmigruje bez výpadku aktuálního provozu, včetně sestavených VPN tunelů. V sekundární lokalitě CMKOS a KZPS je jeden samostatný Cisco ASA firewall bez řešení vysoké dostupnosti.

Z hlediska VPN josu využity technologie IPSec Site-to-Site VPN jako propojení primární a sekundární lokality za účelem replikace dat. Dále je využita technologie SSL Remote Access VPN pro připojení virtuálního serveru v terciální lokalitě k primární lokalitě, případně sekundární lokalitě, také za účelem replikace dat. Další SSL Remote Access VPN přístupy jsou využívány pro vzdálený přístup administrátorů k aktivním prvkům sítě a serverům. Ukončené uživatelské VPN jsou ověřovány pomocí uživatelského jména a hesla v lokální databázi na firewallu. Podporované operační systémy pro SSL VPN jsou Linux RedHat Ent., MAC OS – Intel/PPC, Windows XP/Vista/7 - 32/64 bitové a Windows 8.

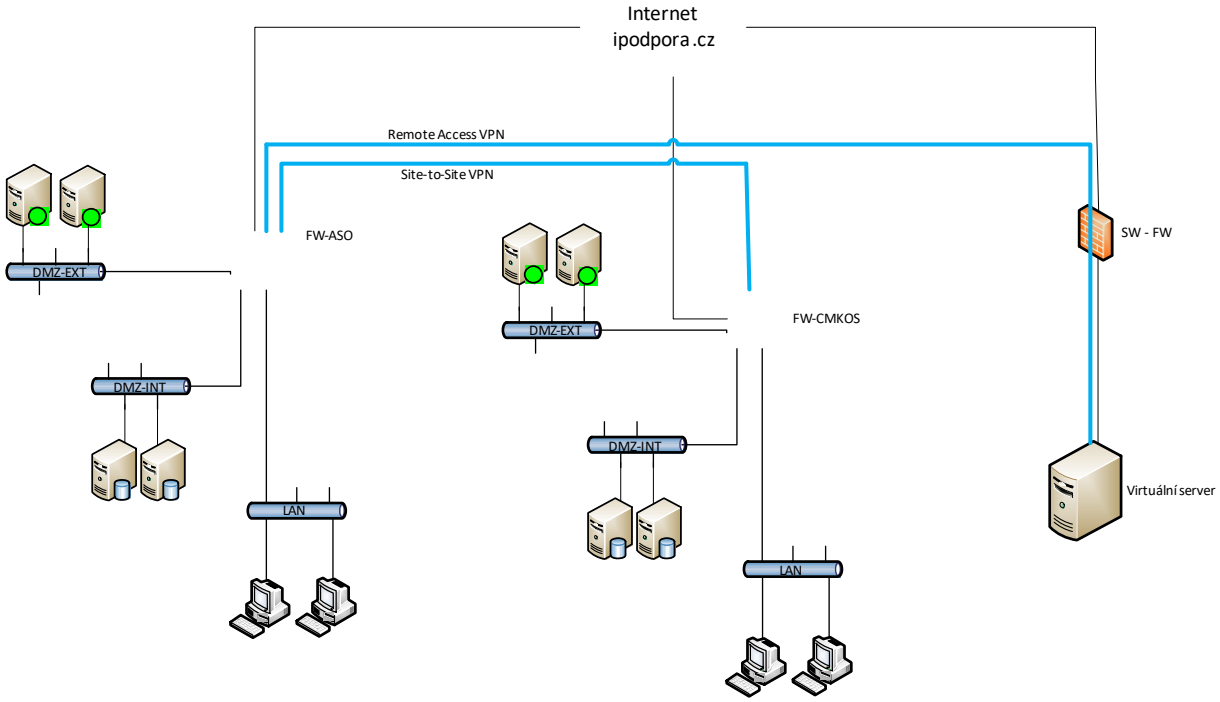
Fyzické zapojení firewallu podporuje redundantní připojení tak, aby se pro každý segment mohla využít dvojice fyzických rozhraní z každého firewallu (vytvoří se tzv. redundantní rozhraní nebo etherchannel). Každé rozhraní v rámci redundant „bundlu" je zapojeno do jiného přepínače pro zvýšení vysoké dostupnosti.

Firewally mají na na sobě ukončené 4 typy segmentů.

-Internet segment pro přístup k ISP
-DMZ segment, kde jsou umístěny frontend servery
-DMZ segment pro backend servery
-LAN segment s uživateli

-Služební failover segment pro synchronizaci konfigurace atd. (pouze primární lokalita)

## 15 Topologie




## 16 Software

Prostředí je virtualizováno s použitím prvků vysoké dostupnosti virtuálních serverů. Nosným OS pro virtualizaci je systém VMware vSphere v edici Essential Plus Kit. Toto řešení vyhovuje provozu nabízené aplikační vrstvy a umožňuje administrátorům provádět běžné činnosti údržby virtualizační platformy za provozu aplikačních virtuálních serverů. Data jsou ukládána a distribuovaná na polích v3700. Systém lze doplnit implementací VMware replikačních technologií a zálohováním, které jsou v použité edici obsaženy.

## 17 Aplikace

Rozsah instalovaných aplikací a jejich vazby jsou předmětem samostatné dokumentace. Podle ní jsou vytvořeny potřebné parametry virtuálních serverů a instalace jejich operačních systémů.