Specifikace služeb a parametrů SLA

Tato Dohoda o úrovni služeb (Service Level Agreement – dále jen SLA) je uzavřena mezi Příjemcem a Poskytovatelem a popisuje způsob zajištění a provozování služby a s ní souvisejících procesů.

1. Popis současného stavu síťové infrastruktury

Zákazník provozuje síťovou infrastrukturu, která se skládá z níže uvedených prvků. U jednotlivých prvků je uveden stručný popis jejich účelu v rámci sítě. Schéma jejího zapojení je uvedeno na obr. 1.

- **Agregační switche** TC1-GWE a TC2-GWE – 2x Cisco Catalyst C9500-24Y4C-A
  - připojují externí sítě
  - řeší směrování – statický routing, PBR, dynamický routing BGP
  - řeší HA – HSRP

- **Core switche** TC1-CORE a TC2-CORE – 2x C9606R-48Y24C-BN-A
  - core síťové prvky pro každou lokalitu – L2 a L3
  - vzájemně propojení mezi lokalitami realizováno jako StackWise Virtual s redundantními propojovacími linkami

- **Access switche** TC1-ACCESS a TC2-ACCESS – 4x C9300L-48T-4X
  - rozšiřuji core switche o metalickou konektivitu

- **Perimetrové firewally** TC1-FTD a TC2-FTD – 2x Cisco FPR3110-NGFW-K9 + management Secure Firewall Management Center (FMC - virtuální appliance)
  - řídí komunikaci mezi interní sítí a externími sítěmi
  - realizují DMZ
  - realizují VPN připojení uživatelů
  - realizují L2L tunely pro připojení externích subjektů
  - realizují IPS/IDS funkce a inspekci procházejícího provozu
  - jsou zapojeny v HA páru

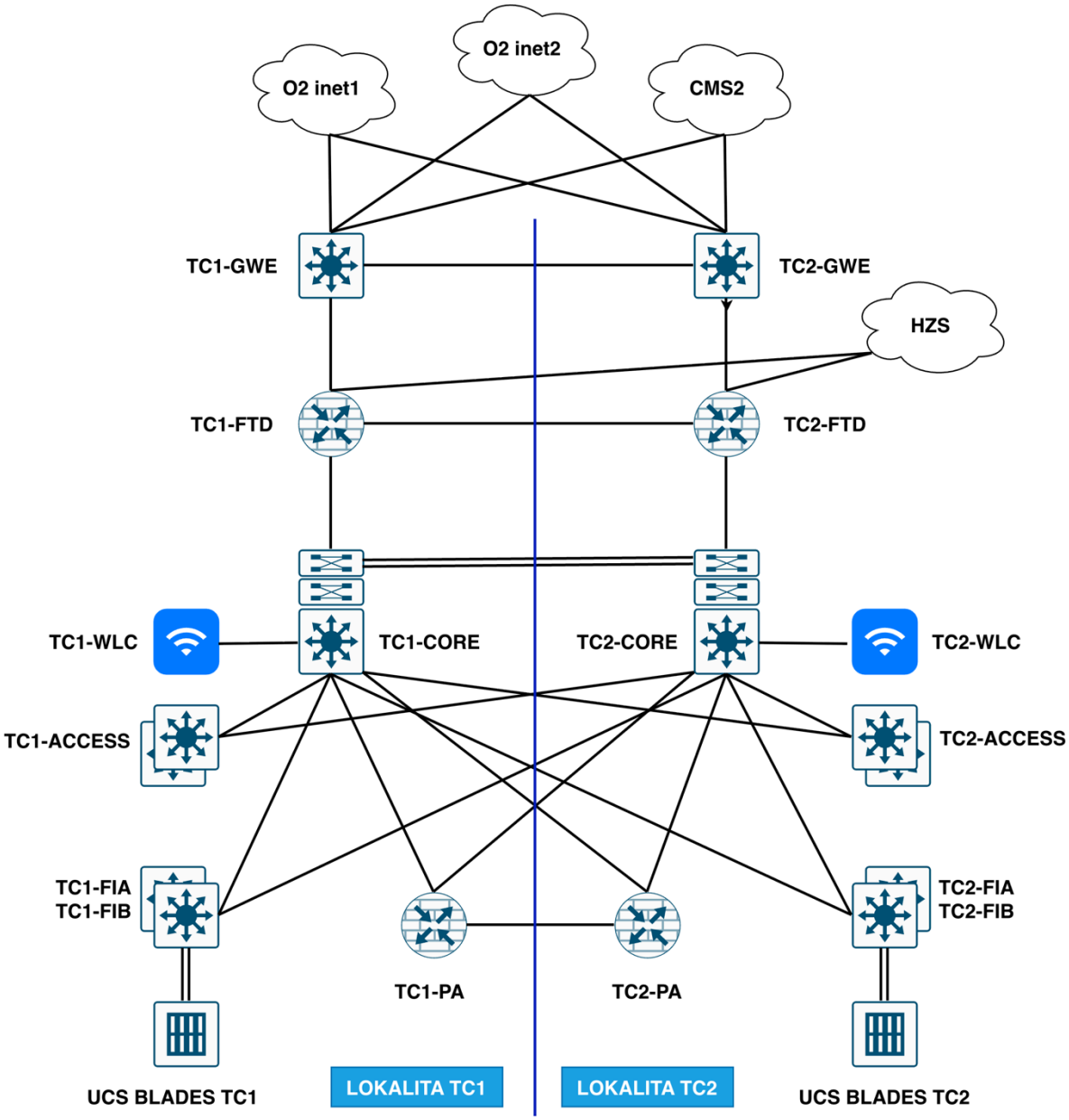
- **Segmentační firewally** TC1-PA a TC2-PA – 2x Palo Alto PAN-PA-3440 + management Panorama (virtuální appliance)
  - řídí komunikaci mezi segmenty interní sítě
  - realizují inspekci provozu
  - jsou zapojeny v HA páru

- **Řadiče bezdrátové sítě** TC1-WLC a TC2-WLC – 2x Cisco Catalyst 9800-L
  - řídí AP
  - jsou zapojeny v HA páru

- **Fibre Channel switche** – 4x Cisc MDS 9132T (DS-C9132T)
  - realizují storage síť pro komunikaci serverové infrastruktury s diskovými úložišti
  - vždy dva prvky tvoří samostatný fabric – HA zapojení

- **Serverová platforma pro virtualizaci** TC1-FIA, TC1-FIB, TC2-FIA, TC2-FIB – 4x Cisco Fabric Interconnect UCS-FI-6454-U

- vždy dva prvky tvoří cluster v rámci lokality – HA zapojení
- FI propojují serverovou platformu s IP TC1a storage sítí



2. Vymezení jednotlivých činností vykonávaných Poskytovatelem v rámci služby

Pro účely vymezení, které konkrétní služby budou realizovány, pro které konkrétní prvky, jsou prvky rozděleny do následujících skupin:

Skupina 1:

- **Agregační switche** TC1-GWE a TC2-GWE
- **Core switche** TC1-CORE a TC2-CORE
- **Access switche** TC1-ACCESS a TC2-ACCESS
- **Perimetrové firewally** TC1-FTD a TC2-FTD + FMC
- **Segmentační firewally** TC1-PA a TC2-PA + Panorama

Skupina 2:

- **Fibre Channel switche**

Skupina 3:

- **Řadiče bezdrátové sítě TC1-WLC a TC2-WLC**
- **Serverová platforma pro virtualizaci** TC1-FIA, TC1-FIB, TC2-FIA, TC2-FIB

Služby požadované pro skupinu 1:

- udržování provozní konfigurace prvků a provádění změn konfigurace dle zadání Příjemce („svěřená správa“)
- konzultace k libovolným tématům týkajícím se prvků
- diagnostika hardwarových závad a součinnost při jejich řešení s výrobcem/dodavatelem
- realizace změn nastavení prvků vedoucích k rozšíření funkcionalit tohoto řešení
- provozování virtuálního serveru na prostředcích Příjemce, který bude sloužit pro uchovávání záloh konfigurací prvků, výměnu souborů (dokumentace) mezi Příjemcem a Poskytovatelem. Údržba serveru bude plně v režii Poskytovatele
- nastavení a kontrola provádění periodických záloh konfigurace
- příprava a údržba Disaster Recovery (DR plán) plánu pro řešení krizových situací (definice postupů obnovy fungování síťové infrastruktury pouze pro realizované prvky)
- provádění činností dle DR plánu v případě nutnosti jeho aktivace
- provádění aktualizací SW prvků, provádění upgradů na nové verze SW prvků (po konzultaci s Příjemcem)
- periodické (minimálně 1x týdně) provádění profylaktické kontroly zdraví prvků na základě analýzy interních logů prvků a využití systémových prostředků (CPU, RAM, síť a podobě)
- periodické sledování (nejméně 1x týdně) informací výrobce prvků o případných bezpečnostních problémech a implementace bezpečnostních záplat/opatření doporučených výrobcem (po konzultaci s Příjemcem)
- vedení provozní dokumentace prvků a její pravidelná aktualizace 1x měsíčně. Dokumentace bude zaznamenávat všechny relevantní změny, které v nastavení prvků proběhly. Dokumentace bude vedena minimálně v rozsahu dle vzoru v kapitole 10
- periodické (1x měsíčně) vytváření reportů o činnosti Poskytovatele, které budou obsahovat zejména následující informace:
    - vyhodnocení plnění SLA na základě vyhodnocení reakcí na požadavky zadané Příjemcem
    - informace o bezpečnostních bulletinech poskytovaných výrobci prvků
    - informace o aktuálních a nově vydaných verzích SW prvků
    - aktuální komunikační matice
    - informace o výsledcích profylaktických kontrol zdraví prvků
- nastavení globálního Read-Only administrátorského přístupu Příjemce k prvkům

- nastavení omezeného Read-Write administrátorského přístupu k vybraným prvkům umožňujícího Příjemci provádět běžné provozní změny (např. nastavování ACL na FW)

Služby požadované pro skupinu 2:

- nastavení a kontrola provádění periodických záloh konfigurace
- konzultace k libovolným tématům týkajícím se prvků
- příprava a údržba Disaster Recovery (DR plán) plánu pro řešení krizových situací (definice postupů obnovy fungování síťové infrastruktury pouze pro realizované prvky)
- provádění činností dle DR plánu v případě nutnosti jeho aktivace
- provádění aktualizací SW prvků, provádění upgradů na nové verze SW prvků (po konzultaci s Příjemcem)
- periodické sledování (nejméně 1x týdně) informací výrobce prvků o případných bezpečnostních problémech a implementace bezpečnostních záplat/opatření doporučených výrobcem (po konzultaci s Příjemcem)
- periodické (1x měsíčně) vytváření reportů o činnosti Poskytovatele, které budou obsahovat zejména následující informace:
    - informace o bezpečnostních bulletinech poskytovaných výrobci prvků
    - informace o aktuálních a nově vydaných verzích SW prvků

Služby požadované pro skupinu 3:

- konzultace k libovolným tématům týkajícím se prvků
- periodické sledování (nejméně 1x týdně) informací výrobce prvků o případných bezpečnostních problémech a implementace bezpečnostních záplat/opatření doporučených výrobcem (po konzultaci s Příjemcem)
- periodické (1x měsíčně) vytváření reportů o činnosti Poskytovatele, které budou obsahovat zejména následující informace:
    - informace o bezpečnostních bulletinech poskytovaných výrobci prvků
    - informace o aktuálních a nově vydaných verzích SW prvků

Rozsah následujících činností bude omezen objemem 12 MD/rok a práce nad tento rámec budou hrazeny na základě samostatných objednávek:

- realizace změn nastavení výše uvedených spravovaných prvků vedoucích k rozšíření jejich funkcionalit

Přehled čerpání MD v rámci ročního období bude součástí reportu o činnosti Poskytovatele.

3. Provozní doba služby

3.1. Provozní doba pro hlášení problémů (zakládání požadavků) je od 00:00 do 24:00 včetně svátků a dnů pracovního volna a klidu (režim 24 x 7 x 365)

3.2. Provozní doba pro plnění této služby a interval pro počítání měřených parametrů (SLA) je od 00:00 do 24:00 mimo svátků a dnů pracovního volna a klidu (režim 24 x 5 x 365) s výjimkou činností uvedených v bodě 3.3

3.3. Provozní doba pro plnění této služby a interval pro počítání měřených parametrů (SLA) pro níže uvedené činnosti je od 00:00 do 24:00 včetně svátků a dnů pracovního volna a klidu (režim 24 x 7 x 365):

- provádění činností dle DR plánů
- řešení reklamací činností realizovaných Poskytovatelem (např. chybně realizovaný požadavek na změnu)

4. Termíny a standardní měřené parametry

4.1. Standardní měřené parametry jsou:
- Doba odezvy
- Doba na odstranění závady či vyřešení požadavku

4.2. Klasifikace doby odezvy a maximální doby na odstranění závady či vyřešení požadavku:

Oblast	Maximální doba odezvy	Maximální doba odstranění závady či vyřešení požadavku
Řešení závad klasifikovaných jako kritické	1 hodiny	4 hodin (tato doba může být u konkrétních požadavků prodloužena po vzájemné dohodě obou stran)
Řešení ostatních závad a požadavků	4 hodiny	24 hodin (tato doba může být u konkrétních požadavků prodloužena po vzájemné dohodě obou stran)
Poskytování konzultací	NBD	3 NBD

5. Pravidla pro klasifikaci závad a požadavků

Klasifikace	Popis
Kritické závady	Za kritickou závadu je považován každý stav, kdy dojde k omezení činnosti Příjemce
Ostatní závady a požadavky	Všechny ostatní závady a požadavky nespadající pod klasifikaci „Kritické závady“

Poskytovatel může po prozkoumání problému navržený stupeň důležitosti požadavku ve spolupráci s Příjemcem překlasifikovat. V případě, že Příjemce nesouhlasí se stanovením klasifikace, provede eskalaci požadavku.

6. Podmínky poskytování služby

- Příjemce poskytne Poskytovateli přístup do systému, který je předmětem této smlouvy, prostřednictvím VPN a sdělí Poskytovateli potřebné přihlašovací údaje. Poskytovatel odsouhlasí s Příjemcem parametry tohoto připojení, při jejich změně se budou strany vzájemně informovat. Pokud bude pro některou z činností vykonávaných Poskytovatelem nutná osobní přítomnost pracovníků poskytovatele u Příjemce, jsou všechny náklady Poskytovatele s tím spojené již zahrnuty v ceně služby a Poskytovatel nemůže požadovat hrazení žádných nákladů s tím souvisejících.

- Příjemce akceptuje, že jeho činnost bude auditována prostřednictvím PIM/PAM řešení Příjemce.

- Příjemce je povinen v případě potřeby zajistit součinnost oprávněné osoby Příjemce (systémový administrátor, popř. jiná oprávněná osoba) a poskytnou po dobu řešení incidentu potřebné přihlašovací údaje do systému.

- Příjemce v souvislosti s nahlášením požadavků uvede veškeré jemu známé okolnosti, pravdivé a nezkreslené informace a jiné údaje, důležité pro úspěšné a včasné poskytnutí služby.

7. Eskalační proces

V případě vzniku nestandardní situace během řešení závady či požadavku je Příjemce oprávněn eskalovat tuto situaci dle následujícího postupu:

1. úroveň manager týmu poskytujícího službu
2. úroveň ředitel společnosti nebo jeho pověřený zástupce

Seznamy a kontaktní údaje oprávněných osob (kontaktní matice), přesná specifikace postupů a další detaily vzájemné komunikace jsou uvedeny v dokumentu Komunikační matice (Příloha č. 5 smlouvy). Aktualizace komunikační matice je prováděna v dokumentu „Report o činnosti poskytovatele“. Stav v dokumentu „Report o činnosti poskytovatele“ je považován za aktuálně platný.

8. Definice pojmů

8.1. **Doba odezvy:** je maximální čas, do kterého musí být zahájeno řešení požadavku či závady. Za zahájení řešení požadavku či závady je považováno odeslání emailové zprávy Příjemci o přiřazení požadavku či závady konkrétnímu řešiteli.

8.2. **Doba vyřešení Kritické závady:** je maximální čas, do kterého musí být závada vyřešena. Tato doba počíná běžet od nahlášení závady Poskytovateli.

Za vyřešení závady se považuje obnovení funkce prvku, který byl závadou postižen, do původního stavu a potvrzení funkčnosti Příjemcem. Do času plnění SLA se nezapočítává čas mezi oznámením o vyřešení závady ze strany Poskytovatele do doby potvrzení Příjemcem.

8.3. **Doba vyřešení ostatních závad a požadavků:** je maximální čas, do kterého musí být požadovaná konfigurační změna provedena nebo závada odstraněna. Tato doba počíná běžet od nahlášení požadavku Poskytovateli.

9. Postupy pro komunikaci

9.1. Komunikace mezi Poskytovatelem a Příjemcem při hlášení závad a požadavků je vždy možná minimálně těmito třemi způsoby:

- prostřednictvím rozhraní webové aplikace dostupné v Internetovém prohlížeči prostřednictvím sítě Internet
- e-mailem na definované e-mailové adresy
- telefonicky na definovaných tel. číslech

9.2. Všechny výše uvedené způsoby komunikace jsou si rovny a zvolená varianta hlášení nemá žádný vliv na povinnost dodržení doby odezvy a doby vyřešení požadavku.

9.3. Veškerá komunikace mezi Poskytovatelem a Příjemcem probíhá v českém jazyce.

10. Definice rozsahu dokumentace

Popis a schéma externí části sítě
- agregační switche TC1-GWE a TC2-GWE
- routing - statický, BGP, PBR
- zapojení konektivit (externích sítí) – IP rozsahy, jejich využití
- IPv6
- hierarchie NTP

Perimetrové firewally a FMC
- DMZ
- VPN
- NAT
- management

Popis a schéma interní část sítě
- 9k6
- segmentační firewally Palo Alto a jejich management
- IP rozsahy, seznam VLAN

Připojení externích sítí
- Popis, schéma, adresace

VPN
- VPN pro uživatele/dodavatele
- popis VPN skupin, adresace
- L2L tunel SUSJK – popis, adresace, schéma

Služební server

- popis, adresace, funkce

Zálohování – popis a nastavení