



Technická specifikace

1 Úvod

Zadavatel požaduje dodání Systému pro zabezpečení síťové komunikace (firewallu), jehož účelem bude ochrana perimetru a bude plnit i funkci segmentačního firewallu, tj. oddělí specifické interní segmenty sítě. Dodání dalších funkcionalit v rámci zvoleného licenčního setu nepředstavuje pro vyhodnocení nabídek žádnou další výhodu.

Základní informace o IT prostředí zadavatele

- Zadavatel disponuje platformou Checkpoint Maestro.
- Zadavatel používá pro přihlášení do správy jednotlivých systémů PAM (Privileged Access Managment) Aricoma ID.
- Zadavatel provozuje virtuální prostředí na platformě VMware.

Lokality, ve kterých budou systém a technologie aplikován a provozován:

Nemocnice následné péče Horažďovice, s.r.o., Blatenská 314, 34101 Horažďovice

Nemocnice následné péče Svatá Anna, s.r.o., Kyjovská 607, 34815 Planá

2 Parametry systému – požadavek na funkce

- HW platforma pouze formou HW appliance
- Propustnost minimálně 4 Gbps pro plnou inspekci (IPS, Antivir, AntiBot, sandboxing) a 9 Gbps NGFW. Parametry se vztahují na každou appliance zvlášť v rámci HA řešení
- Konektivita každé HW appliance minimálně 2x10GbE SFP+ interface
- Minimálně 2x napájecí zdroj na každou HW appliance
- Licenční set musí obsahovat IPS, URL filtering, DNS security, Antivirus, ochranu před zero-day zranitelnostmi, včetně emulace souborů
- Podpora VLAN, možnost připojení TRUNK interface
- technická podpora minimálně po dobu plánované životnosti 5 let od data dodání
- licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů
- režim HA v módu Active-Standby, složený ze dvou zařízení
- site-to-site VPN pomocí protokolu IPSec
- podpora identifikace aplikací napříč všemi porty/protokoly
- podpora identifikace aplikací na nestandardních portech
- podpora vytváření bezpečnostních pravidel na základě uživatelských identit.

3 Implementace systému

- Instalace všech HW komponent do racku pomocí dodaného příslušenství pro montáž
- Zapojení optické a metalické kabeláže, zapojení napájení
- Konfigurace přístupových údajů a napojení na centrální management
- Konverze stávajících firewall objektů a politik na nové řešení
- Bezpečnostní hardening řešení.



Akceptační kritéria nasazení Systému:

- Nastavení bezpečnostních pravidel definovaných zadavatelem
- Úspěšné provedení testovaných scénářů pro ověření plné funkcionality systému
- Propojení systémů a správa pomocí platformy Checkpoint Maestro.
- Funkční hardening řešení.

4 Požadavek na integraci a sdílení

Zadavatel provozuje pro centrální řízení datového provozu mezi síťovými rozhraními Maestro Hyperscale Orchestrator. Zadavatel požaduje, aby dodávaný systém byl napojen na toto rozhraní a přebíral technická nastavení.

5 Licence

Licenční pokrytí musí respektovat definované parametry jakožto nejmenší možnou množinu funkcionalit. Všechny části systému musí být pokryty podporou výrobce a všemi požadovanými licencemi/subskripcemi na dobu pěti let.

6 Požadavky na bezpečnost, zálohování a správu

Systém bude provozován v režimu 24×7, servisní výpadky provozu pro provedení aktualizací bude prováděno dle oboustranně odsouhlaseného harmonogramu a v předem stanovených časových termínech.

Systém musí umožnit aplikovat režim řízení a nastavení více úrovní přístupových oprávnění pro uživatele systému. Jednomu uživateli může být přiřazeno více rolí.

Systém musí umožnit nastavení různých úrovní přístupů pro jednotlivé role uživatelů. Nastavit jednotlivým uživatelům povolenou funkcionalitu a rozsah dat, ke kterým mohou přistupovat.

Systém musí umožnit opravu klíčových dat pouze uživateli s příslušnými právy.

Systém musí umožnit zaznamenání aktivity uživatele a změn dat.

Zadavatel provádí zálohování pomocí stávajícího systému Veeam, ať už aplikační nebo databázové části. Dodavatel v podané nabídce předloží a popíše způsob zálohování a archivace dat a Systému s přihlédnutím k zálohovacímu systému zadavatele.

Dodavatel předloží jako součást dokumentace k Systému zpracovaný návrh dokumentace pro případ havárie celého nebo některé části systému – Disaster Recovery plán, s popisem nezbytných postupů a činností pro úplné obnovení jeho běhu. S každou novou verzí, případně významnou změnou prostředí, musí proběhnout jeho revize a případně aktualizace.

Využívané webové služby musí umožnit zabezpečení pomocí SSL certifikátu zadavatele.

Veškeré nastavení všech součástí Systému je nutné provádět v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB) a Vyhlášky č. 82/2018 Sb. (Vyhláška o kybernetické bezpečnosti).