**Příloha č. 2 - Technická specifikace**

k veřejné zakázce s názvem

Výzva č. 8: Rozšíření kybernetické bezpečnosti v Krajské zdravotní, a.s. DC3 – Síťová hardware mikrosegmentace

**Verifikační tabulka – minimální požadavky –** **Mikrosegmentační switch s podporou vysoce výkonného**

**firewallu – 4ks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Počet** | **Popis položky** | **Splňuje**  **Ano/ne** | **Nabídnutá hodnota parametrů (vlastností)** |
| **1** | **mikrosegmentační switch s podporou rychlostí 40/100 Gbps v počtu minimálně 6 portů 40/100Gbps zadavatel dále připouští možnost dodání více síťových prvků.** |  |  |
|  | **Switchovací výkon minimálně 3.2 Tbps** |  |  |
|  | **Routovací výkon minimálně 2000 Mpps** |  |  |
|  | **Počet záznamů MAC adres v paměti minimálně 98000** |  |  |
|  | **Počet indikativních rout minimálně 130000 pro ipv4** |  |  |
|  | **Minimálně 25000 pravidel v Access listu / Firewall listu pro IPv4 tak IPv6** |  |  |
|  | **Plná podpora Jumbo frame o minimální velikosti 9000 B** |  |  |
|  | **Podpora LACP IEEE 802.3ad** |  |  |
|  | **Podpora 802.1Q** |  |  |
|  | **Protokol pro šíření VLAN nastavení - MVRP dle IEEE 802.1ak či VTP** |  |  |
|  | **Podpora technologie VXLAN jak ve statické implementaci tak v dynamické pomocí BGP (eVPN) a to jak pro IPv4 tak pro IPv6. Implementace VXLAN musí byt schopna pracovat s plovoucí bránou v anycast provozu. V provozu VXLAN musí být podporován i multicast.** |  |  |
|  | **Plná podpora protokolů BGP (BGP-4), OSPF, MPLS, RIPv2 a RIPng.** |  |  |
|  | **Podpora RFC 3176** |  |  |
|  | **Podpora API a programování skriptů v jazyce Python** |  |  |
|  | **Packet bufer minimálně 32MB** |  |  |
|  | **First Hop Redundancy Protokol** |  |  |
|  | **Policy-based routing** |  |  |
|  | **IGMPv1/v2/v3** |  |  |
|  | **IP Multicast (PIM SM, SSM)** |  |  |
|  | **IPv6 Multicast (MLDv1 & v2, PIM SM, SSM)** |  |  |
|  | **Podpora uRPF** |  |  |
|  | **Podpora IEEE 802.1D, IEEE 802.1S,** **EEE 802.1W** |  |  |
|  | **Podpora QOS** |  |  |
|  | **Podpora NAT** |  |  |
|  | **MPLS tuneling (L3VPN, L2VPN, pseudowire)** |  |  |
|  | **MPLS FRR maximálně 40ms** |  |  |
|  | **Podpora virtuálních směrovacích tabulek (VRF)** |  |  |
|  | **Minimální počet virtuálních směrovacích tabulek je vyšší než 100** |  |  |
|  | **Podpora Network load balancing nezavisle na operačním systému** |  |  |
|  | **Firewall s propustností 800Gbps ve skutečném mikrosegmentovaném provozu** |  |  |
|  | **Firewall musí mít k dispozici minimálně dva fyzické ASIC CPU o frekvenci minimálně 2,95 GHz dále pak vlastní úložiště o minimální kapacitě 64 GB.** |  |  |
|  | **Základní funkcionalita Firewallu v tomto switchi je oddělení jednotlivých prostředků zadavatele (virtualizační platformy i operační systémy) do takzvaných mikro-celků ( mikrosegmentů) a zajištění propagace těchto celků na úrovni technologie privatVLAN či podobné, minimálně podporované platformy HyperV, ProxMox, ESXi.** |  |  |
|  | **Podpora Firewall pravidel jak ve formě ACL (IPv4 i IPv6) tak pravidel AGL s detekcí aplikace tak statických FW pravidel segment / segment s možností nasazení inspekce a využití signaturních detekcí** |  |  |
|  | **Firewall musí zároveň podporovat včasnou detekci nestandardního a/nebo nežádoucího toku v provozu, automatizované terminace tohoto toku a upozornění obsluhy pro vyšetření daného incidentu.** |  |  |
|  | **Zadavatel připouští že analýza provozu může být získávána z operačního systému pomocí SW agenta který však nesmí spotřebovat víc než 4% výkonu přidělených prostředků (CPU / RAM). Agent musí být k dispozici minimálně pro operační systémy Linux (Debian, Ubuntu, Rocky), Unix (OpenBSD), MS Windows Server (2016, 2019, 2022, 2025), MS Windows (11)** |  |  |
|  | **Centrální monitoring všech událostí s napojením na systém centrální správy a logovacích nástrojů zadavatele. Zadavatel požaduje integraci do SIEM QRadar minimálně na úrovni odesílání logů a jejich parsingu.** |  |  |
|  | **Podpora iSCSI, Lossless iSCSI, RDMAoCE v2, Express NVMe over Fabrics v bezztrátovém provozu.** |  |  |
|  | **Propojený boxů do logického celku takzvaného stacku, virtuálního chassis či podobného celku.** |  |  |
|  | **Aktualizace řídícího software tak aby nedošlo k výpadku celého logického celku.** |  |  |
| **1** | **Napájení minimálně 2 x Hot-plug, Redundant Power Supply (1 + 1), 230V s minimální účinností 91% při 100% zatížení** |  |  |
| **1** | **Oddělený management port LAN s podporu rychlostí 10/100/1000 Mbps** |  |  |
| **1** | **Oddělený management port pro sériovou komunikaci** |  |  |
| **1** | **Licence pro použití všech portů a funkcí bez funkčního, časového i kapacitního omezení rovněž bez funkčního omezení.** |  |  |
| **1** | **Chlazení zepředu dozadu, osazení ventilačními jednotkami v maximálním možném počtu, který umožňuje daný switch a pro potřeby redundance chladícího výkon** |  |  |
| **1** | **Veškerého instalačního příslušenství pro montáž do racku.** |  |  |
| **1** | **Veškeré příslušenství pro zapojení do logického celku** |  |  |
| **1** | **Vzdálený management ve formě CLI (SSHv2 AES), SNMP v2c či SNMPv3 (AES). Autorizace do zařízení pomocí mechanizmů Radius, TACACS+, Podpora Simple File Transfer Protocol (SFTP).** |  |  |
| **1** | **Podpora na 12 měsíců - Next Business Day (oprava do následujícího pracovního dne s evidencí chyb a reakcí podpory 24/7 s odezvou do 4 hodin)** |  |  |
| **1** | **Propojovací sada kabelů pro vytvoření logického celku o kapacitě 100Gbps a vysoké dostupnosti.** |  |  |

**Verifikační tabulka – Aplikace (SW) pro správu mikrosegmentační switch s podporou vysoce výkonného firewallu – 1ks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Počet** | **Popis položky** | **Splňuje**  **Ano/ne** | **Nabídnutá hodnota parametrů (vlastností)** |
| **1** | **Software centrální správy mikrosegmentační switch s podporou vysoce výkonného firewallu bez funkčního a časového omezení.** |  |  |
|  | **Možnost provozu aplikace ve virtuálním prostředí KVM tak na fyzickém HW (HW není součástí této VZ)** |  |  |
|  | **Aplikace by měla umožňovat pracovat ve vysoké dostupnosti** |  |  |
|  | **V jedné instanci je nutné umožnit spravovat více logických celků switchů bez licenčního omezení** |  |  |
|  | **Platforma musí být pomocí API schopna komunikovat jak se switchi tak s virtualizačními hosty/platformami** |  |  |
|  | **Management aplikace musí běžet ve formě webového rozhraní, aplikace v jazyce JAVA nejsou povoleny. Webová aplikace musí podporovat prohlížeč Chrome na všech platformách.** |  |  |
|  | **Software musí být schopen reportovat do systém centrální správy a logovacích nástrojů zadavatele dále informovat obsluhu o stavu jednotlivých prvků a logických celků, a to přehledně a jednoznačně. Zadavatel požaduje integraci do SIEM QRadar minimálně na úrovni odesílání logů a jejich parsování.** |  |  |
|  | **SW musí indikovat stavy všech připojených infrastruktur** |  |  |
|  | **V rámci rozhraní musí být role uživatel schopen definovat všechny pravidla jak ACL tak Firewall, automatizovaně řídit provoz, analyzovat incidenty provádět aktualizace jednotlivých prvků i rozhraní samotného.** |  |  |
|  | **SW musí podporovat průvodce konfigurace jednotlivých významných funkcionalit a musí mít integrovanou nápovědu nezávislou na přístupu k internetu ze strany zadavatele.** |  |  |
|  | **SW musí umožnit řízené zapisování pravidel jak okamžitě, tak plánované.** |  |  |
|  | **SW musí umožnit vytvářet skupiny uživatelů jako v lokální databázi tak s napojením na Radius, TACACS+ či LDAPS.** |  |  |
| **1** | **Podpora na 12 měsíců - Next Business Day (oprava do následujícího pracovního dne s evidencí chyb a reakcí podpory 24/7 s odezvou do 4 hodin)** |  |  |
| **1** | **Školení pro 5 uživatelů certifikované výrobcem pro implementaci zařízení.** |  |  |

**Při nesplnění akceptačních a obchodních podmínek si objednatel vyhrazuje zboží nepřevzít.**

**Požadavky na předmět plnění uvedené v tomto dokumentu jsou závazné, jejich nedodržení bude považováno za nesplnění zadávacích podmínek s následkem vyloučení dodavatele z účasti v zadávacím řízení.**

**-----------------------------------------------------------------------------------------------------------------**

**Dodavatel prohlašuje, že jím nabízené plnění splňuje všechny požadavky uvedené v této Příloze č. 2 - Technická specifikace:**

**V ……(vyplní účastník)……… dne …(vyplní účastník)…**

**Za společnost**

**………………………(vyplní účastník)………………………………**

**Osoba oprávněná jednat jménem či za účastníka (pozice, titul, jméno, příjmení)**

**……………………(vyplní účastník)……………………………….**