NENROE RADAR #02

VEŘEJNÉ ZAKÁZKY ZA 5 MINUT



UKÁZKOVÝ RODNÝ LIST

Dodávka a implementace firewallu pro městský úřad

Autentický výstup vytvořený AI platformou NENROE

POZNÁMKA K VÝSTUPU

Příloha obsahuje ukázky pracovních výstupů vytvořených AI platformou NENROE na základě jednoduchého a podrobného zadání modelové veřejné zakázky.

Účelem je ukázat rozdíly v rozsahu a podrobnosti návrhu. Text není odborně validovanou technickou specifikací ani vzorem zadávací dokumentace. Některé požadavky mohou být nepřesné, vzájemně rozporné nebo nepřiměřené a před případným použitím vyžadují odborné posouzení.

CO BY PŘED POUŽITÍM UPRAVILI NAŠI ODBORNÍCI?

Oblast	Validace / Oprava
Technická specifikace	**Potenciálně nepřiměřené a diskriminační požadavky.**
Kybernetická bezpečnost	**Odkazy na povinnosti podle vyhlášky**
Hodnocení nabídek	**Nejednoznačný bodovací model**
Smluvní podmínky	**Drobné rozpory v harmonogramu**

UKÁZKA RODNÉHO LISTU

PŘEDMĚT OBECNĚ (JEDNODUCHÉ ZADÁNÍ)

Předmětem veřejné zakázky je dodávka nového firewallu včetně jeho instalace, konfigurace a uvedení do provozu pro zabezpečení komunikační sítě a připojení k internetu Města XY. Součástí plnění je také zajištění servisní podpory a bezpečnostních aktualizací po dobu 5 let. Řešení musí splňovat požadavky zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v režimu nižších povinností.

NIPEZ kódy: 32420000-3

Kódy NIPEZ a CPV

- NIPEZ: 32420000-3 - Síťová zařízení
  - CPV: 32420000-3 - Síťová zařízení
- NIPEZ: 32422000-7 - Síťové komponenty
- NIPEZ: 32427000-2 - Síťové systémy

PŘEDMĚT OBECNĚ (DETAILNÍ ZADÁNÍ)

Předmětem veřejné zakázky je dodávka nového firewallu včetně jeho instalace, konfigurace, začlenění do stávající síťové infrastruktury, uvedení do provozu, předání dokumentace a zaškolení administrátorů. Součástí plnění bude také zajištění servisní podpory, licencí a bezpečnostních aktualizací po dobu 5 let. Zakázka je zaměřena na zabezpečení komunikační sítě městského úřadu v souladu s požadavky zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a vyhlášky č. 410/2025 Sb.

NIPEZ kódy: 32420000-3

Kódy NIPEZ a CPV

- NIPEZ: 32420000-3 - Síťová zařízení
  - CPV: 32420000-3 - Síťová zařízení
- NIPEZ: 32422000-7 - Síťové komponenty
- NIPEZ: 32424000-1 - Síťová infrastruktura
- NIPEZ: 32427000-2 - Síťové systémy
- NIPEZ: 32428000-9 - Modernizace/vylepšení sítě

PŘEDMĚT DETAILNĚ (JEDNODUCHÉ ZADÁNÍ)

Předmětem plnění je dodávka, instalace, konfigurace a uvedení do provozu **Next Generation Firewall (NGFW)** pro zabezpečení komunikační sítě Města XY, včetně servisní podpory a bezpečnostních aktualizací po dobu **5 let**. Řešení musí splňovat požadavky zákona č. **264/2025 Sb., o kybernetické bezpečnosti** v režimu nižších povinností.

1. Požadavky na dodávku a implementaci

- **Hardwarové a softwarové komponenty**:
  - Dodávka firewallu s podporou **NGFW funkcionalit** (deep packet inspection, aplikace a uživatelské kontroly, ochrana před malwarem, IPS/IDS, sandboxing).
  - Licence pro **100 uživatelů** a pokrytí všech nezbytných informačních systémů městského úřadu.
  - Kompatibilita s existující síťovou infrastrukturou (vč. integrace s aktivními síťovými prvky).
- **Instalace a konfigurace**:
  - Fyzická instalace zařízení do stávající sítě.
  - Nastavení **zón, pravidel, VPN, a segmentace sítě** dle požadavků kybernetické bezpečnosti.
  - Konfigurace **high availability** (pokud je požadována redundance).
  - Integrace s **SIEM systémem** (pokud je zadavatelem využíván).
  - Testování funkčnosti a **penetrační test** před uvedením do provozu.
- **Uvedení do provozu**:
  - Školení pro správce sítě (min. **2 osoby**) v rozsahu **8 hodin** (teorie + praktické ukázky).
  - Dokumentace **konfiguračních souborů, síťových schémat a bezpečnostních politik**.
  - Předání **provozní a správcovské dokumentace** v českém jazyce.

2. Servisní podpora a údržba

- **24/7 monitorování** a reakce na kritické incidenty (do **4 hodin** od nahlášení).
- **Bezpečnostní aktualizace** (firmware, signature databáze) **do 72 hodin** od vydání výrobcem.
- **Helpdesk a hotline** s **SLA**:
  - Reakční doba na požadavek: **2 hodiny** (pracovní dny 8:00–16:00).
  - Řešení incidentů dle priorit (kritické: **4 h**, vysoké: **8 h**, střední: **24 h**, nízké: **48 h**).
- **Legislativní podpora** (zajištění souladu s **264/2025 Sb.** a dalšími relevantními normami).
- **Roční audity** bezpečnostní konfigurace (1x ročně).

3. Technické specifikace

- **Propustnost**: Minimálně **1 Gbps** (s možností rozšíření).
- **Počet současných spojení**: **≥ 500 000**.
- **Podpora IPv6**.
- **Certifikace**: **Common Criteria EAL4+** nebo ekvivalent.
- **Zálohování konfigurace** (automatické, denní).

4. Povinnosti dodavatele

- Zajištění **plynulé migrace** ze stávajícího řešení (minimalizace výpadků).
- **Záruka** na hardware: **5 let** (vč. náhrady zařízení do **24 hodin** při kritické poruše).
- **Reporting**: Měsíční zprávy o bezpečnostních událostech a aktualizacích.

PŘEDMĚT DETAILNĚ (DETAILNÍ ZADÁNÍ)

Předmětem plnění veřejné zakázky je **pořízení, implementace a servis firewallu** pro zabezpečení komunikační sítě Města XY, včetně následujících konkrétních činností a dodávek:

1. Dodávka firewallu

- **Typ zařízení**: Firewall kategorie **Next Generation Firewall (NGFW)** s podporou pokročilých funkcí (IPS, IDS, aplikační kontrola, anti-malware, anti-bot, SSL inspekce, sandboxing pro detekci neznámých hrozeb).
- **Hardwarové požadavky**:
  - Propustnost firewallu (dle RFC 3511, 2544, 2647, 1242): **minimálně 1 000 Mbps** (upřesnit dle konkrétních potřeb a stávající infrastruktury).
  - Propustnost IPS: **minimálně 500 Mbps**.
  - Propustnost NGFW (firewall + IPS + aplikační kontrola): **minimálně 500 Mbps**.
  - Propustnost Threat ochrany (firewall + IPS/IDS + aplikační kontrola + anti-malware + anti-bot): **minimálně 250 Mbps**.
  - Počet nových spojení za vteřinu (CPS): **minimálně 10 000**.
  - Počet současných spojení: **minimálně 500 000**.
  - Počet fyzických síťových rozhraní: **minimálně 4x 10/100/1000baseT** (upřesnit dle potřeb).
  - Podpora **dual stack IPv4/IPv6**.
  - Podpora **redundance dvou zařízení v režimu Active-Standby se stavovou synchronizací** (pokud je požadována vysoká dostupnost).
- **Bezpečnostní požadavky**:
  - **URL filtering** na základě kategorizace (pokrytí minimálně 85 % Alexa Top 1M sites).
  - **Detekce a řízení síťových aplikací** (minimálně 7 500 rozpoznávaných aplikací).
  - **Ochrana proti neznámým hrozbám**: Emulace souborů ve virtuálním sandbox prostředí (podporované typy: powerpoint, word, excel, pdf, exe, archivy zip/tar/7z/rar).
  - **SSL inspekce** včetně HTTPS kategorizace.
  - **Site-to-Site VPN** s autentizací pomocí certifikátu (podpora algoritmů: AES-128, AES-256, SHA-256, AES-XCBC).
  - **Remote Access VPN** (licence pro minimálně 50 souběžných uživatelů, upřesnit dle potřeb).
  - **Blokace SQL Injection a CSS útoků** v celé URL a HTML body.
  - **Ochrana proti SNI spoofing** v rámci HTTPS inspekce.
  - **Podpora Captive portálu** s lokální autentizací uživatelů a autentizací vůči Active Directory.
  - **Integrované diagnostické nástroje** pro detekci chyb systému.
  - **Automatické aktualizace** ochran (IPS, Anti-bot, Anti-Virus, aplikační kontrola).
  - **Podpora Zero-touch deployment** prostřednictvím cloudového portálu.
  - **Bezpečnostní logy** ukládány na fyzicky oddělenou management platformu.
  - **Maximální počet publikovaných zranitelností OS (CVE) za poslední 3 roky**: **max. 15**.
  - **Automatické vypnutí IPS ochrany** v případě přetížení HW (využití CPU nebo paměti nad definovanou prahovou hodnotu).
- **Správa a monitorování**:
  - Správa zařízení pomocí **webové konzole** (kompatibilní s prohlížeči Google Chrome, Microsoft Edge, Mozilla Firefox).
  - **Centrální správa** z on-prem nebo cloudového managementu.
  - **Integrované monitorovací dashboardy** (pohledy: aktivní zařízení, infikovaná zařízení, VPN tunely, spojení).
  - **Mobilní aplikace** pro monitorování a správu (podpora Android/iOS, sledování stavu zařízení, síťových portů, upozornění na nové/infikované zařízení).
  - **Podpora linux nástrojů** (SCP, BASH, VI, TOP) a spouštění skriptů třetích stran.

  - **Podpora verzování bezpečnostních politik** a generování rozdílových reportů.
- **Podpora protokolů a funkcí**:
  - NAT, PAT.
  - Dynamic DNS.
  - Filtrování MAC adres.
  - DNS proxy.
  - Agregace fyzických portů (LACP).
  - Podpora modifikace velikosti MTU.
  - Konfigurace rozhraní: Switch mode, Bridge mode, Bond (Link Aggregation), VPN Tunnel, VLAN Alias.
  - Podpora **MTA agenta** pro skenování souborů (Anti-virus, Zero-day ochrana).
  - **Přidávání vlastních IOC indikátorů** (IP, MD5, URL) manuálně nebo přes API.
  - **Firewall performance analyzer** (min. top 10 spojení a jejich % konzumace HW zdrojů).
  - **Odstranění aktivního obsahu** (makra, javascript) ze souborů (podporované typy: MS Office, PDF, JPEG, BMP, PNG, TIFF, GIF).
  - **Zablokování prvního pokusu o stažení zero-day malware** přes SMTP, SMTPs, HTTP, HTTPS.
- **Výrobce**: Musí být uveden v **Gartner Magic Quadrant for Enterprise Network Firewalls** za poslední 3 roky v kvadrantu **Leader**.

2. Implementace a konfigurace

- **Instalace a fyzické zapojení** firewallu do stávající síťové infrastruktury.
- **Konfigurace**:
  - Nastavení základních síťových parametrů (IP adresy, VLAN, routing).
  - Konfigurace bezpečnostních politik (Access Policy, Threat Policy) dle "best-practices".
  - Nastavení **SSL inspekce** (včetně HTTPS kategorizace).
  - Konfigurace **VPN** (Site-to-Site, Remote Access).
  - Nastavení **URL filtering** a aplikační kontroly.
  - Integrace s **Active Directory** pro autentizaci uživatelů.
  - Nastavení **Captive portálu** pro hosty.
  - Konfigurace **logování** a monitorování (včetně odesílání logů na externí systém).
  - Nastavení **automatických aktualizací** bezpečnostních signatur.
- **Testování**:
  - Ověření funkčnosti všech konfigurovaných služeb.
  - Test **propustnosti** a výkonu zařízení.
  - Test **failoveru** (pokud je použita redundance).
  - Test **VPN spojení** a autentizace.
- **Dokumentace**:
  - **Technická dokumentace** (schéma zapojení, konfigurace, bezpečnostní politiky).
  - **Uživatelská příručka** pro správu a monitorování.
  - **Provozní dokumentace** (postupy pro běžnou údržbu, řešení problémů).
  - **Bezpečnostní dokumentace** (popis implementovaných opatření, doporučení pro další zabezpečení).

3. Zaškolení administrátorů

- **Cíl**: Zaškolení **minimálně 2 administrátorů** městského úřadu pro samostatnou správu a údržbu firewallu.
- **Rozsah**:
  - **Teoretická část**: Principy fungování NGFW, bezpečnostní politiky, detekce hrozeb.

  - **Praktická část**:
    - Správa zařízení přes webové rozhraní a centrální management.
    - Konfigurace základních i pokročilých funkcí (VPN, SSL inspekce, aplikační kontrola).
    - Monitorování a analýza logů.
    - Řešení běžných problémů a reklamací.
    - Aktualizace firmware a bezpečnostních signatur.
  - **Délka**: **Minimálně 16 hodin** (8 hodin na administrátora, nebo společné školení).
- **Forma**: Prezenční nebo online (dle dohody), s možností praktických cvičení na testovacím prostředí.

4. Servisní podpora a údržba

- **Doba podpory**: **5 let** od předání a převzetí zařízení.
- **Rozsah podpory**:
  - **24/7 telefonická a e-mailová podpora** (v pracovních dnech 8:00–17:00, mimo pracovní dobu pouze pro kritické závady).
  - **Reakční doba**:
    - Kritické závady (výpadek služby): **do 2 hodin** od nahlášení.
    - Významné závady (omezená funkčnost): **do 4 hodin** od nahlášení.
    - Ostatní závady: **do 24 hodin** od nahlášení.
  - **Oprava závad**: Bezplatné odstranění vad v rámci záruční doby (24 měsíců od předání).
  - **Aktualizace**:
    - **Bezpečnostní aktualizace** (IPS, Anti-Virus, Anti-Bot, aplikační kontrola) **automaticky** nebo manuálně dle dohody.
    - **Firmware aktualizace** (minimálně 1x ročně, nebo dle potřeby).
  - **Licence**:
    - Všechny potřebné licence pro **plnou funkčnost firewallu** (včetně pokročilých funkcí) po dobu **5 let**.
    - Licence pro **Remote Access VPN** (upřesnit počet uživatelů).
    - Licence pro **sandboxing** a **threat intelligence**.
- **SLA (Service Level Agreement)**:
  - **Dostupnost podpory**: 99,5 % v pracovních hodinách.
  - **Doba obnovy služby (MTTR)**: **Maximálně 4 hodiny** pro kritické závady.
  - **Reportování**: Měsíční zprávy o stavu zařízení, vyřízených požadavcích a aktualizacích.

5. Další požadavky

- **Bezpečnost dodavatelského řetězce**:
  - Dodavatel musí prokázat, že **všechny komponenty firewallu** (HW i SW) pocházejí od důvěryhodných výrobců s **certifikovaným dodavatelským řetězcem**.
  - **Vyloučení rizikových dodavatelů**: Dodavatel nesmí používat komponenty od výrobců, kteří jsou na sankčních listech EU/USA nebo mají známé bezpečnostní rizika.
- **Dlouhodobá podpora výrobce**:
  - Firewall musí být **podporován výrobcem po dobu minimálně 5 let** od data pořízení.
  - Výrobce musí poskytovat **pravidelné bezpečnostní aktualizace** a **technickou podporu**.
- **Kompatibilita**:
  - Firewall musí být **kompatibilní** se stávající síťovou infrastrukturou městského úřadu (upřesnit typy zařízení, protokoly atd.).
  - Podpora **stávajících síťových protokolů** (např. IPv4/IPv6, VLAN, OSPF/BGP).
- **Záruka**:
  - **24 měsíců** na hardware (včetně náhradních dílů).
  - **Bezplatná výměna** vadného zařízení do **5 pracovních dnů** od nahlášení závady.

- **Environmentální požadavky**:
  - **Spotřeba energie**: Maximální spotřeba **< 500 W** (upřesnit dle konkrétního modelu).
  - **Hlučnost**: **< 50 dB** (pro umístění v kancelářích).
  - **Teplotní odolnost**: Provozní teplota **0–40 °C**, skladovací teplota **-20–70 °C**.

6. Požadavky dle zákona č. 264/2025 Sb. a vyhlášky č. 410/2025 Sb.

- Firewall musí splňovat **požadavky na zabezpečení komunikační sítě** dle **§ 5–10 zákona č. 264/2025 Sb.** (kybernetická bezpečnost).
- **Monitorování a logování**:
  - **Centralizované logování** všech bezpečnostních událostí.
  - **Ukládání logů** po dobu **minimálně 1 roku** (dle vyhlášky č. 410/2025 Sb.).
  - **Automatické upozornění** na bezpečnostní incidenty (e-mail, SMS, integrace s SIEM).
- **Bezpečnostní politiky**:
  - **Předdefinované politiky** pro veřejnou správu (např. blokace nebezpečných webových stránek, omezení přístupu k citlivým datům).
  - **Možnost přizpůsobení** politik dle specifických potřeb města.
- **Audity a compliance**:
  - **Podpora pro audity** (generování reportů o dodržování bezpečnostních opatření).
  - **Dokumentace pro NÚKIB** (přehled implementovaných opatření, konfigurace, logy).

7. Dodávka a předání

- **Místo dodání**: Síťové centrum městského úřadu (upřesnit adresu).
- **Termín dodání**: **Do 30 dnů** od podpisu smlouvy (upřesnit dle rozsahu zakázky).
- **Předání**:
  - Předávací **protokol** podepsaný oběma stranami.
  - **Ověření funkčnosti** všech požadovaných funkcí.
  - **Předání dokumentace** (technická, uživatelská, provozní).
  - **Zaškolení administrátorů** před nebo během předávání.

8. Údaje vyžadující upřesnění zadavatelem

- **Konkrétní technické parametry** (propustnost, počet rozhraní, počet VPN uživatelů atd.) – závisí na **stávající infrastruktuře** a **požadavcích města**.
- **Počet a typ licencí** (dle počtu uživatelů a požadovaných funkcí).
- **Požadavky na redundanci** (Active-Standby, Active-Active).
- **Integrace se stávajícími systémy** (např. SIEM, Active Directory, monitoring).
- **Specifické bezpečnostní požadavky** (např. blokace určitých zemí, aplikací atd.).

DOBA PLNĚNÍ (JEDNODUCHÉ ZADÁNÍ)

- **Dodávka a instalace hardware**: Do **30 kalendářních dnů** od podpisu smlouvy.
- **Konfigurace, testování a uvedení do provozu**: Do **60 kalendářních dnů** od podpisu smlouvy.
- **Servisní podpora a údržba**: **5 let** od data uvedení do provozu (zahrnuje průběžné aktualizace a monitoring).

DOBA PLNĚNÍ (DETAILNÍ ZADÁNÍ)

- **Zahájení plnění**: **Do 15 dnů** od podpisu smlouvy (včetně přípravy dokumentace a plánování implementace).
- **Dodávka a instalace firewallu**: **Do 30 dnů** od podpisu smlouvy.
- **Konfigurace a testování**: **Do 45 dnů** od podpisu smlouvy.
- **Zaškolení administrátorů**: **Do 50 dnů** od podpisu smlouvy.
- **Předání a převzetí**: **Do 55 dnů** od podpisu smlouvy.
- **Servisní podpora a údržba**: **5 let** od data předání a převzetí.

Odůvodnění:

Doba plnění vychází z porovnání s obdobnými zakázkami (např. **Hasičský záchranný sbor Pardubického kraje** – dodávka 14 ks firewallů s implementací a servisem trvala **2 měsíce** od zahájení do předání). V tomto případě se jedná o **1 firewall** pro menší organizaci (100 zaměstnanců), proto je doba plnění zkrácena na **~2 měsíce** pro dodávku a implementaci. Servisní podpora je standardně poskytována po dobu **5 let**, což odpovídá běžné praxi u NGFW řešení.

PŘEDPOKLÁDANÁ HODNOTA

4 000 000 Kč bez DPH

DRUH ŘÍZENÍ

Druh veřejné zakázky: DODÁVKY

Režim veřejné zakázky: PODLIMITNÍ

Druh zadávacího řízení: Zjednodušené podlimitní řízení

Tato zakázka je podlimitní (4 000 000 Kč bez DPH, hranice pro podlimitní zakázky u tohoto typu zadavatele je 3 000 000 Kč bez DPH) a nevyžaduje složitý předvýběr dodavatelů. Zjednodušené podlimitní řízení umožňuje efektivní a rychlejší postup při zachování transparentnosti.

TYP SMLOUVY

Typ smlouvy: Smlouva o dílo

Odůvodnění: Předmětem zakázky je dodávka firewallu včetně jeho instalace, konfigurace, uvedení do provozu a dlouhodobé servisní podpory. Smlouva o dílo je vhodná, protože zahrnuje jak dodání věci (hardware), tak provedení prací (instalace, konfigurace) a zajištění výsledku (funkční firewall s podporou).

KVALIFIKACE

Základní způsobilost

Dodavatel musí splňovat základní způsobilost podle § 74 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“). Je-li dodavatelem právnická osoba nebo účastní-li se zadávacího řízení prostřednictvím pobočky závodu, vztahují se podmínky základní způsobilosti na osoby uvedené v § 74 odst. 2 až 4 ZZVZ.

Prokázání základní způsobilosti

Ve zjednodušeném podlimitním řízení prokazuje dodavatel splnění základní způsobilosti způsobem podle § 53 odst. 4 ZZVZ čestným prohlášením, pokud zadavatel v zadávací dokumentaci nestanoví jinak.

Vyhradí-li si to zadavatel v zadávací dokumentaci, prokazuje dodavatel splnění základní způsobilosti doklady podle § 75 ZZVZ. Doklady se předkládají v prostých kopiích a mohou být nahrazeny jednotným evropským osvědčením pro veřejné zakázky podle § 87 ZZVZ.

Doklady prokazující základní způsobilost podle § 74 musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení.

Dodavatel není povinen předkládat doklady, které si zadavatel může opatřit z informačního systému veřejné správy. Tyto doklady lze nahradit odkazem na příslušný informační systém veřejné správy nebo obdobný systém jiného členského státu umožňující neomezený dálkový přístup.

Splnění základní způsobilosti lze rovněž prokázat výpisem ze Seznamu kvalifikovaných dodavatelů podle § 228 ZZVZ nebo platným certifikátem vydaným v rámci systému certifikovaných dodavatelů podle § 234 a násl. ZZVZ, a to v rozsahu údajů, které tyto doklady prokazují.

Zadavatel je oprávněn kdykoliv v průběhu zadávacího řízení požadovat předložení originálů nebo úředně ověřených kopií dokladů o kvalifikaci.

Profesní způsobilost

Dodavatel musí prokázat oprávnění podnikat v oblasti dodávek hardwaru a softwaru pro síťové zabezpečení, zejména v rozsahu odpovídajícímu předmětu veřejné zakázky. Dále musí předložit výpis z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis vyžaduje.

Ekonomická kvalifikace

Ekonomická kvalifikace není povinně vyžadována.

Technická kvalifikace (JEDNODUCHÉ ZADÁNÍ)

Dodavatel musí prokázat zkušenosti s dodávkou, instalací, konfigurací a servisní podporou **Next Generation Firewall (NGFW)** řešení v posledních 3 letech před zahájením zadávacího řízení. Konkrétně musí předložit:

- **Seznam referencí** (minimálně 2 realizované zakázky) s obdobným předmětem plnění, včetně kontaktů na zadavatele pro ověření.
- **Popis technického řešení** pro alespoň jednu z referencí, včetně specifikace hardwaru, softwaru, licencí a poskytnutých služeb (instalace, konfigurace, školení, servis).
- **Doklad o certifikaci** dodavatele nebo jeho zaměstnanců od výrobce NGFW (**např. Fortinet, Palo Alto Networks, Cisco, Check Point nebo ekvivalentní**), který potvrzuje odbornou způsobilost pro implementaci a správu těchto systémů.

Technická kvalifikace (DETAILNÍ ZADÁNÍ)

Dodavatel musí prokázat splnění technické kvalifikace podle **§ 79 odst. 2 zákona č. 134/2016 Sb.** následujícími způsoby:

- **Reference na obdobné zakázky**:
  - Předložení **seznamu významných dodávek** (minimálně 2) realizovaných v posledních **3 letech** před zahájením zadávacího řízení, které se týkaly:
    - Dodávky a implementace **Next Generation Firewall (NGFW)** řešení.
    - Dodávky síťových bezpečnostních zařízení s obdobnými technickými parametry (propustnost, počet rozhraní, podporované funkce).

        - Poskytování servisní podpory a údržby pro bezpečnostní zařízení po dobu minimálně **3 let**.
    - Každá reference musí obsahovat:
        - Název objednatele a kontaktní údaje pro ověření.
        - Popis dodávky (včetně technických parametrů a rozsahu plnění).
        - Datum realizace a celkovou hodnotu zakázky (bez DPH).
- **Odborná způsobilost týmu**:
    - Dodavatel musí prokázat, že disponuje **kvalifikovaným týmem** s odbornými znalostmi v oblasti:
        - Konfigurace a správy **NGFW** (např. certifikace od výrobců jako **Palo Alto Networks, Fortinet, Cisco, Check Point**).
        - Implementace bezpečnostních opatření dle **zákona č. 264/2025 Sb.** a **vyhlášky č. 410/2025 Sb.**
        - Správa a monitorování síťové infrastruktury.
    - Doložení **certifikátů nebo školení** pro klíčové členy týmu (např. **CCNA Security, PCNSE, Fortinet NSE 4-7**).
- **Technická kapacita**:
    - Dodavatel musí prokázat, že má **technické a personální kapacity** pro:
        - Dodávku, instalaci a konfiguraci firewallu v požadovaném rozsahu.
        - Zajištění **24/7 servisní podpory** (včetně reakčních dob dle SLA).
        - Poskytování **bezpečnostních aktualizací** a údržby po dobu **5 let**.

HODNOCENÍ NABÍDEK

Hodnocení nabídek bude provedeno **podle poměru ceny a kvality** s následujícími kritérii a váhami:

Kritéria hodnocení a jejich váhy:

Kritérium	Váha	Metoda vyhodnocení
Celková nabídková cena	70 %	Metoda: **Nejnižší cena** získá plný počet bodů (100 %). Ostatní nabídky obdrží body poměrně podle vzorce: *(Nejnižší cena / Nabídková cena) × 100*. Cena se posuzuje **bez DPH**.
Technická úroveň nabízeného řešení	20 %	Bodové hodnocení dle následujících podkritérií: ▪ **Propustnost a výkonnost** (max. 5 bodů): Splnění nebo překročení požadované propustnosti **1 Gbps** a počtu současných spojení **≥ 500 000**. ▪ **Funkčnost NGFW** (max. 5 bodů): Podpora **deep packet inspection, IPS/IDS, sandboxing, aplikace a uživatelské kontroly**. ▪ **Certifikace** (max. 5 bodů): Přítomnost certifikace **Common Criteria EAL4+** nebo ekvivalentní. ▪ **Redundance a high availability** (max. 5 bodů): Nabídka řešení s **high availability** (pokud požadováno zadavatelem). **Maximální počet bodů**: 20. **Přepočet na váhu**: *(Získané body / 20) × 20 %*.
Kvalita servisní podpory	10 %	Metoda: Bodové hodnocení dle následujících podkritérií: ▪ **Reakční doby** (max. 5 bodů): Splnění požadovaných SLA (kritické incidenty do **4 hodin**, vysoké do **8 hodin** atd.).

		▪ **Dostupnost podpory** (max. 3 body): **24/7 monitorování** a hotline. ▪ **Záruční podmínky** (max. 2 body): **5letá záruka** na hardware a náhrada zařízení do **24 hodin** při kritické poruše. **Maximální počet bodů**: 10. **Přepočet na váhu**: *(Získané body / 10) × 10 %*.

Celkové hodnocení:

Nabídka s **nejvyšším součtem vážených bodů** (cena + technická úroveň + servis) bude vybrána jako nejvhodnější.
V případě **shodného počtu bodů** bude upřednostněna nabídka s **nižší celkovou cenou**.

Obchodní podmínky

Obchodní a jiné podmínky

- **Dodací podmínky**: Dodání firewallu a souvisejících licencí do **14 dnů** od podpisu smlouvy. Instalace, konfigurace a uvedení do provozu do **30 dnů** od dodání hardware.
- **Způsob převzetí plnění**:
  - Předání hardware proti **převzetí protokolu** s ověřením technického stavu.
  - **Testování funkčnosti** (včetně penetračního testu) před definitivním převzetím.
  - **Protokol o uvedení do provozu** podepsaný oběma stranami.
- **Platební podmínky**:
  - **Záloha 30 %** po podpisu smlouvy.
  - **40 %** po dodání a instalaci hardware.
  - **20 %** po úspěšném testování a uvedení do provozu.
  - **10 %** po předání dokumentace a školení.
- **Smluvní pokuty**:
  - **Prodlení s dodáním**: 0,1 % z ceny zakázky za každý den prodlení (max. 10 %).
  - **Nedodržení SLA**: 0,5 % z roční ceny servisu za každé porušení kritických SLA (max. 5 % ročně).
  - **Nedodržení kybernetických požadavků**: 1 % z celkové ceny za každé zjištěné porušení zákona č. **264/2025 Sb.**
- **Výpovědní doba**: **3 měsíce** s písemným upozorněním. Při porušení smlouvy možnost okamžité výpovědi.
- **Pojištění odpovědnosti dodavatele**: Minimálně **5 000 000 Kč** (odpovídá předpokládané hodnotě zakázky).
- **SLA požadavky**:
  - **24/7 monitorování** a reakce na kritické incidenty do **4 hodin**.
  - **Bezpečnostní aktualizace** do **72 hodin** od vydání výrobcem.
  - **Helpdesk**: Reakční doba **2 hodiny** (pracovní dny 8:00–16:00).
- **Ochrana osobních údajů (GDPR)**: Dodavatel musí prokázat soulad s **Nařízením (EU) 2016/679** a zajistit ochranu zpracovávaných údajů.
- **Kybernetická bezpečnost**: Dodržení zákona č. **264/2025 Sb.** v režimu nižších povinností, včetně pravidelných auditů (1x ročně).
- **Mlčenlivost**: Závazek mlčenlivosti o všech obchodních a technických informacích zadavatele po dobu **5 let** od ukončení smlouvy.
- **Ochrana duševního vlastnictví**: Dodavatel zaručuje, že dodané řešení neporušuje práva třetí strany a předá veškerá práva k dokumentaci zadavateli.

- **Exit plán**: Dodavatel je povinen předat veškerou dokumentaci, konfigurace a školení pro plynulý přechod k novému dodavateli při ukončení smlouvy.

DODAVATELÉ

1. O2 Czech Republic a.s.
2. Aricoma Systems a.s.
3. Microshop, s.r.o.

PŘÍLOHY

- Zadávací dokumentace
- Čestná prohlášení dodavatele – k mezinárodním sankcím, ke střetu zájmu

Nepovinné přílohy:

- Čestné prohlášení dodavatele k prokázání základní a profesní způsobilosti
- Čestné prohlášení k prokázání technické kvalifikace
- Smlouva o dílo
- Seznam poddodavatelů

Výstupy a dokumenty platformy NENROE jsou generovány nástrojem umělé inteligence (AI), mají informativní povahu a mohou být neúplné či nepřesné. Výstupy nejsou právně závazné, nepředstavují odborné poradenství ve smyslu § 2950 občanského zákoníku ani právní služby dle § 1 odst. 2 zákona o advokacii. Před použitím je povinná lidská validace – kontrola a schválení odpovědnou osobou. Výstupy nesmí být použity k plně automatizovanému rozhodování ani jako jediný podklad pro rozhodnutí s právními účinky. Autoři a provozovatelé NENROE neodpovídají za škody způsobené použitím informací z aplikace v rozporu s tímto upozorněním. Data jsou ukládána a zpracovávána výhradně v EU. Pro námitky či dotazy kontaktujte equica@equica.cz.