|  |  |
| --- | --- |
| **Zadávací PODMÍNKY** **k veřejné zakázce malého rozsahu v souladu s § 6, § 27 a § 31 Zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „zákon“)** | |
| Název zakázky: | **Dodávka bezpečnostního řešení NGFW (Next-Generation Firewall) v konfiguraci vysoké dostupnosti** |
| **Název zadavatele:** | Statutární město Ostrava |
| **IČ zadavatele:** | 00845451 |
| **Kontaktní adresa zadavatele:** | Prokešovo náměstí 8, 729 30 Ostrava |
| **Kontaktní osoba zadavatele:** | Ing. Martin Honajzer, OVANET a.s., Hájkova 1100/13, 702 00 Ostrava - Přívoz |
| **Telefon:** | 555 135 650 |
| **E-mail:** | honajzer@ovanet.cz |
| 1. Vymezení předmětu veřejné zakázky | |
| Předmětem veřejné zakázky je dodávka a implementace redundantního bezpečnostního řešení s dedikovaným systémem pro správu a reporting. Hlavním cílem projektu je doplnění stávajících bezpečnostních platforem o funkce NGFW, zejména s ohledem na aplikační a webovou inspekci. Zadavatel předpokládá další rozšiřování systému a proto je kladem vysoký důraz na modularitu a granularitu výkonu bezpečnostní platformy.    Schéma požadovaného bezpečnostního řešení NGFW  Síťová topologie je navržena, tak aby každý dodávaný NGFW měl síťové rozhraní do všech segmentů vnitřní sítě a ke všem případným linkám internetového poskytovatele. Virtuální management, pak musí mít přístup ke všem firewallům, buď pomocí nezávislých přepínačů, nebo přímým propojením. Stávající FW, ISP routery ani páteřní přepínače nejsou součástí zakázky.   |  |  | | --- | --- | | **Požadované položky** | **Počet** | | NGFW appliance (včetně HW + SW) | min. 2 ks | | Virtual management appliance (pouze SW) | min. 1 ks |   **NGFW appliance (nejméně 2 ks)**  Zadavatel požaduje možnost připojení nejméně dvou nezávislých připojení k síti internet. Z tohoto důvodu vyžaduje, aby navržené řešení umožňovalo rozkládání odchozí komunikace mezi výše zmíněná připojení. Rozkládání zátěže je požadováno jak pro kryptovanou, tak i nekryptovanou komunikaci. Požadavkem je možnost nastavení kvality služeb, na základě šířky pásma a latence linky poskytovatele. Oba NGFW musí umožňovat alespoň základní možnosti vysoké dostupnosti a to v režimech active/active a active/pasive. Rozkládání zátěže lze řešit pomocí přidaného dedikovaného hardware, avšak z bezpečnostních důvodů není možné vysokou dostupnost řešit jinak, než pomocí přímo integrované funkce NGFW. Vzhledem k umístění firewallů na perimetru sítě je požadována podpora následujících směrovacích protokolů: BGP4 (dle RFC 1771, 1963, 1966, 1997, 2918, 2545 a 2858), OSPFv3 (dle RFC 2740), RIP verze dva s autentizací (dle RFC 1723). Zadavatel do budoucna zvažuje nasazení multicastu což vyžaduje, aby firewally podporovaly IGMPv3 (dle RFC 33761), PIM (dle RFC 4601, 46011 a 3973) a dále DVMRP (dle RFC 10751). V rámci navrhovaného řešení jsou požadovány tyto základní bezpečnostní funkce NGFW: řízení přístupu, kryptování komunikace, NAT, sledování a logování spojení s detailem na uživatelské jméno v Active Directory zadavatele, IPS, verifikace TCP sekvence, dynamické VPN, podpora asynchronních spojení, podpora synchronních spojení, podpora minimálně pěti prvků v rámci režimu vysoké dostupnosti, podpora virtuálních sítí (dle IEE 802.1Q), ochrana proti spoofingu v interní síti a možnost spuštění nástroje pro správu v rámci vlastního firewallu (webové rozhraní, příkazová řádka).  Provedení NGFW appliance je možné pomocí dedikovaného hardware, nebo virtuálních appliance na fyzickém serveru. Zadavatel požaduje v obou případech nejméně 4 aktivní jádra na každé instanci NGFW a dále možnost rozšíření o čtyři další jádra. Zadavatel chápe a připouští, že v případě rozšíření, může vzniknout požadavek na dodatečný hardware. Cena dodatečného hardware nesmí překročit 20% z ceny nabízeného řešení. Pro splnění předchozího požadavku zadavatel připouští trade-in programy výrobců, pokud dojde k požadovanému rozšíření a budou splněny všechny body specifikace. Pokud se zadavatel rozhodne přejít z varianty čtyři plus čtyři aktivní jádra na variantu osmi aktivních jader na jedné instanci NGFW, není možné, aby vznikly další náklady na SW licence. Uchazeč musí všechny potřebné softwarové náklady (licence, subskripce, služby, podpora apod.) k provozování řešení 4+4 a nebo 8 zahrnout do nabídkové ceny.  **IPS (Intrusion Prevention System)**  Pro efektivní ochranu komunikace vyžaduje zadavatel nasazení IPS. Základním požadavkem na metody filtrace je přítomnost signatur zranitelností a exploitů, validace protokolů a to až do úrovně aplikační vrstvy, detekce anomálií, analýza na základě chování a korelace mezi těmito metodami. Ochrana v reálném čase musí obsahovat detekci alespoň klientských a serverových zranitelností, exploitů, zneužití protokolu, odchozí malware komunikace, pokusy o tunelování a detekci pomocí generických algoritmů nespoléhající čistě na signatury.  **Logování**  Pro efektivní analýzu událostí je požadována funkce identifikace jednotlivých záznamů a jejich přiřazení k uživatelským účtům v Active Directory. Zadavatel požaduje podporu nejméně, Windows server 2008 (SP2, 32 a 64 bit), Windows server 2012 v libovolné licenční edici. Párované logy musí obsahovat minimálně informace z logů firewallu, antiviru a filtrování URL.  **Řízení webových aplikací**  Pro řízení použití webových aplikací uživateli, požaduje zadavatel minimálně funkce identifikace webových aplikací včetně sociálních sítí s možností povolit, zakázat anebo omezit jejich použití. Konfiguraci musí být možné nastavit pro jednotlivé uživatele i uživatelské skupiny dle Active Directory. Aby bylo možné pravidla efektivně nastavovat, musí být filtry rozpoznávající sociální sítě členěny do kategorií. Zadavatel požaduje, aby kategorie obsahovaly minimálně tyto množiny Instant Messaging, Peer 2 Peer, sílení dat, Hlas a Video. Kategorie hlas a video může být sloučena dohromady.  **Filtrování URL**  Pro omezení přístupů uživatelů komunikujících z lokální sítě zadavatele k internetu, požaduje zadavatel, aby firewall umožňoval funkci filtrování webových stránek na základě URL. Zadavatel vyžaduje, aby firewall obsahoval buď interně, nebo pomocí přístupu do virtualizovaného redundantního prostředí výrobce, databázi s URL seřazenými dle kategorií tak, aby tým zadavatele mohl efektivně povolit/zakázat či omezit přístup k URL. Filtrována musí být i URL přistupována pomocí SSL zabezpečené komunikace s možností nastavení výjimky. Stejně jako u Řízení webových aplikací požaduje zadavatel podporu filtrování URL i pro Web 2.0.  **Antivirus**  Firewall musí být vybaven antivirovým systémem pro inspekci provozu. Zadavatel požaduje, aby antivirus byl postaven na systému s celosvětovou instalovanou bází korporátních síťových firewallů. Je vyžadována databáze signatur o škodlivém kódu a škodlivých webových stránkách. Databáze musí být dynamicky aktualizována podle potřeby, alespoň jednou denně. Firewall musí být schopen zastavit provoz, jež identifikuje jako škodlivý, s možností notifikace a vytvoření výjimky. Kontrolován musí být alespoň http, HTTPS a SMTP provoz. A to i v případě přesměrování portů.  **Antispam**  Zadavatel požaduje funkci Antispam na firewallu. Cílem je ochránit E-mail servery proti DOS a buffer overflow útokům. Dále pak ochránit uživatele před nevyžádanou elektronickou komunikací formou e-mailu. Zadavatel požaduje nasazení Antispam řešení, bez nutnosti jakéhokoliv specializovaného software na klientské stanici. Filtraci příchozí pošty musí být možné provést alespoň na základě vstupní zdrojové adresy, výsledku kontrolu obsahu zprávy a pomocí negativního i positivního přístupového seznamu. Minimální množina kontrolovaných protokolů je POP3 a SMTP.  **Antiboot**  Pro ochranu proti distribuovaným útokům formou internetových botů, požaduje zadavatel, aby byl firewall vybaven ochranným mechanismem pro detekci a zastavení útoků tohoto typu. Cílem je ochránit zadavatele, před útoky z internetu. Také však omezit riziko, že by se koncové stanice zadavatele staly zdrojem útoku. Funkce musí podporovat integrovanou databázi infikovaných adres a také analytické algoritmy pro behaviorální analýzu provozu jednotlivých stanic. Cílem analytické části je odhalení šíření jednotlivých botů a také připojení k tzv. command a controll serverům.  **Emulace hrozeb a jejich odstranění**  Pro zajištění efektivní aplikační ochrany požaduje zadavatel, aby NGFW byl vybaven také funkcí emulace a odstranění hrozeb. Není možné tuto funkci provádět na jiné appliance pokud nebude zajištěna korelace s ostatními službami přímo na úrovni NGFW. Nikoliv zpětně na úrovni log managementu či SIEMu. Zadavatel požaduje podporu operačního systému Windows 7 a vyšších a produktů z rodiny MS Office a Adobe Acrobat Reader. Cílem je zajistit identifikaci dokumentu, emulaci hrozby, odstranění hrozby a následné sdílení bezpečného dokumentu. Požadavky na funkci platí, i pokud je komunikace šifrována pomocí TLS či SSL.  Informace mezi jednotlivými moduly (antivir, antispam,…) firewallu musí být korelovány a jednotlivé moduly musí společně komunikovat k dosažení vysoké úrovně zabezpečení. Zadavatel nezbytně nepožaduje, aby byly všechny funkce v jednom fyzickém zařízení, ale z důvodů optimalizace datového centra požaduje, aby uchazeč dbal na co možná nejlepší optimalizaci velikosti a spotřeby instalovaných fyzických zařízení.  **Dedikovaný management**  Zadavatel požaduje jeden dedikovaný management pro potřeby správy, sběru a korelace logů z jednotlivých firewallů. Zadavatel připouští nasazení log managementu a Security Information and Event Manageru. Pro potřeby budoucího rozšíření musí dedikovaný management podporovat režim vysoké dostupnosti a interní úložiště o velikosti minimálně 15 TB. Cílem je poskytnout efektivní zobrazení události za pomocí přehledných grafů, časových os, v případě geografické informace, v interaktivní mapě. Maximální počet událostí je předpokládán na dva tisíce za vteřinu. Minimální podporovaný počet uživatelů komunikujících z lokální sítě je pět tisíc. Dedikovaný management musí umožnit zobrazení informací v reálném čase a import informací třetích stran pomocí tzv. parseru (minimálně od výrobců stávajícího hardware Cisco). Důraz je kladen hlavně na interaktivitu celého systému, tak aby bylo možné efektivně procházet jednotlivá zobrazení pomocí vnitřních odkazů. Zadavatel vyžaduje, aby dedikovaný management umožňoval generování a export reportů jak z předdefinovaných šablon, tak v uživatelsky upravené formě. Zadavatel požaduje, aby systém disponoval možností uložení všech logů po dobu alespoň jednoho měsíce.  **Prostředí zadavatele**  Je postaveno převážně na technologiích společností Cisco Systems, Hewlett Packard Enterprise, VMware a Microsoft. Primárním firewallem je Cisco ASA, která bude poptávanému řešení předřazena. Hlavní virtualizační platforma zadavatele je postavena na VMware NSX, kde bude také provozován virtuální management. Pokud bude uchazeč potřebovat licence pro virtualizaci, je povinen je zahrnout do nabídky řešení. Pokud bude uchazeč používat jinou virtualizaci než VMware, je povinen do nabídky zahrnout také oficiální certifikační školení výrobce na danou virtualizační platformu.  **Podpora a služby**  Zadavatel požaduje záruku v délce trvání tří let zahájenou od předání HW zadavateli. Součástí záruky musí být všechny signatury, aktualizace a služby nutné k bezproblémovému provozování řešení zadavatelem. V případě selhání HW nebo software požaduje zadavatel odstranění vady v místě dodání a instalace v režimu 8x5 NBD.  Před finální akceptací řešení požaduje zadavatel zaškolení zástupců zadavatele a předání dokumentace k implementovanému řešení.  *Další podmínky plnění předmětu veřejné zakázky jsou uvedeny v  požadavcích na obsah smlouvy ze strany zadavatele – příloha č. 1 zadávací dokumentace.* | |
| 1. Místo plnění veřejné zakázky | |
| Místem předání plnění této zakázky je sídlo zadavatele, tj. Prokešovo nám. 8, 729 30 Ostrava, Magistrát města Ostrava, odbor projektů IT služeb a outsourcingu a lokalita Hájkova 1100/13, 702 00 Ostrava-Přívoz. | |
| 1. Způsob hodnocení nabídek | |
| Nabídky budou hodnoceny podle jejich ekonomické výhodnosti. **Ekonomická výhodnost nabídek bude hodnocena podle nejnižší nabídkové ceny bez DPH.** | |
| 1. Požadavky na způsob zpracování nabídkové ceny, platební podmínky | |
| Uchazeč stanoví nabídkovou cenu za celé plnění veřejné zakázky.  **Nabídková cena** **bez DPH** bude cenou nejvýše přípustnou. Do nabídkové ceny zahrne uchazeč veškeré práce či související služby, nezbytné pro kvalitní provedení plnění.  Zadavatel požaduje, aby uchazeč v nabídce uvedl nabídkovou cenu za celkové plnění jako cenu v Kč v tomto členění:   * nabídková cena bez DPH, * samostatně DPH s příslušnou sazbou a * nabídková cena s DPH.   **Platební podmínky:**  Zálohy nejsou přípustné. Doba splatnosti daňových dokladů bude stanovena minimálně na 14 kalendářních dnů ode dne doručení daňového dokladu zadavateli.  Podrobnosti platebních podmínek jsou uvedeny v požadavcích na obsah smlouvy ze strany zadavatele | |
| 1. Obchodní podmínky | |
| Obchodní podmínky jsou vymezeny požadavky na obsah smlouvy ze strany zadavatele, které jsou uvedeny v příloze č. 1 zadávací dokumentace. | |
| 1. Podmínky, při jejichž splnění je možno překročit výši nabídkové ceny | |
| Zadavatel nepřipouští překročení nabídkové ceny, vyjma sazeb DPH. | |
| 1. Pokyny pro zpracování nabídky | |
| Nabídka bude předložena v jednom vyhotovení, v listinné formě a v českém jazyce.  Uchazeč použije pořadí dokumentů uvedené v následujících bodech tohoto článku zadávací dokumentace.   1. Krycí list nabídky - pro sestavení krycího listu uchazeč použije přílohu č. 2 Zadávací dokumentace. 2. Obsah nabídky. Nabídka bude opatřena obsahem s uvedením čísel stránek u jednotlivých oddílů (kapitol) a zabezpečena proti manipulaci s jednotlivými listy. 3. Doklady prokazující splnění kvalifikace dle bodu VIII. Zadávací dokumentace (Kvalifikační předpoklady). 4. Písemný návrh smlouvy podepsaný osobou oprávněnou podepisovat, a to stanoveným způsobem. Oprávnění k podpisu včetně jeho způsobu dokládá uchazeč příslušným oprávněním (např. výpis z obchodního rejstříku, plná moc). Písemný návrh smlouvy bude zpracován v rozsahu požadavků na obsah smlouvy ze strany zadavatele, které jsou součástí zadávací dokumentace. Smlouva nepodléhá režimu obchodního tajemství podle ust. § 504 zákona č. 89/2012 Sb., občanský zákoník. 5. Prohlášení uchazeče o seznámení se s odkazy ve smlouvě podepsané oprávněnou osobou (příloha č. 3 Zadávací dokumentace). 6. Ostatní | |
| 1. Kvalifikační předpoklady | |
| Profesní kvalifikační předpoklady:   * příslušné oprávnění k podnikání vztahující se k předmětu veřejné zakázky, * aktuální výpis z obchodního rejstříku, jste-li do tohoto rejstříku zapsáni,   Technické kvalifikační předpoklady:   * zadavatel požaduje, aby bezpečnostní řešení bylo ověřeno praxí, výrobce nabízeného řešení musí mít alespoň jedno zastoupení v NSS Labs NGFW group testu 2016 s hodnocením alespoň 99% security effectiveness. Zadavatel nepožaduje, aby se jednalo o identický model, uchazeč však doplní čestné prohlášení dodavatele, že daný prvek dosahuje stejných bezpečnostních kvalit jako výrobek testovaný (v NSS Labs NGFW group testu 2016), * uchazeč musí být registrovaným partnerem všech výrobců, jejichž řešení dodává bez stanovení úrovně s odkazem na webové stránky výrobce, kde lze uvedené partnerství ověřit. | |
| 1. Místo a termín pro doručení nabídek | |
| Místo pro podání nabídek:  Poštou na adresu: **OVANET a.s., Hájkova 1100/13, 702 00 Ostrava – Přívoz** nebo  osobně doručit tamtéž do sídla společnosti OVANET a.s. v hodinách Po - Pá 8:00 – 17:00  **Termín pro podání nabídek** je stanoven nejpozději do **25.10.2016, 10:00 hodin.** | |
| 1. Další podmínky, požadavky a informace zadavatele | |
| 1. Náklady spojené s účastí v zadávacím řízení nese každý účastník sám. 2. Zadavatel nepřipouští variantní řešení nabídky. 3. Nabídka uchazeče bude písemná v uzavřené obálce opatřené adresou uchazeče a bude označena: **Veřejná zakázka – „Dodávka NGFW firewal“** - **NEOTVÍRAT!** Nabídky je možno podat nejpozději do konce lhůty pro podávání nabídek. 4. V případě, že zadávací podmínky obsahují požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty a vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, umožňuje použití i jiných, kvalitativně a technicky obdobných řešení, které však musí být jednotně administrovatelné a zcela kompatibilní v rámci stávajícího IT vybavení. 5. Zadavatel si vyhrazuje právo veřejnou zakázku zrušit. 6. Zadavatel si vyhrazuje právo nehodnotit nabídku uchazeče, jehož cena bude posouzena jako mimořádně nízká. 7. Nabídka nesplňující zadávací podmínky nebude zadavatelem hodnocena. 8. Předpokládaná cena této veřejné zakázky činí 1 990 tis. Kč bez DPH. 9. S ohledem na výši předpokládaných nákladů se nejedná o zadávací řízení dle zákona č. 134/2016 Sb., o veřejných zakázkách, ve znění pozdějších předpisů. | |
| 1. Přílohy | |
| Požadavky na obsah smlouvy ze strany zadavatele – příloha č. 1  Krycí list nabídky – příloha č. 2  Prohlášení uchazeče o seznámení se s odkazy ve smlouvě – příloha č. 3 | |