Příloha č. 1 zadávací dokumentace ve veřejné zakázce

**Technická specifikace předmětu zakázky (Technický list)**

pro Část 2 VZ

**Pozn. zadavatele: Dodavatel v nabídce předloží níže uvedené tabulky, v nichž uvede splnění nebo nesplnění technických požadavků zadavatele. V případě nesplnění kteréhokoliv z požadovaných parametrů bude nabídka účastníka vyloučena z další účasti ve veřejné zakázce.**

# Požadované parametry, funkce, vlastnosti – Nástroj pro ochranu integrity komunikačních sítí - Implementace redundantní bezpečnostní hardware platformy s pokročilými funkcemi Next Generation Firewall

## Technická specifikace

Zadavatel požaduje dodávku Firewall cluster HW boxů a licence pro SW firewall do stávajícího virtualizačního prostředí za účelem zajištění ochrany jak perimetru, tak interní sítě a zajištění bezpečného datového provozu mezi pracovišti Karviná, Orlová a Mizerov. Zadavatel dále požaduje zachování vysoké dostupnosti pro obě lokality – pracoviště Karviná – Ráj a pracoviště Orlová. Zachování vysoké dostupnosti pro pracoviště Mizerov není zadavatelem požadováno.

Zadavatel připouští pouze tuto variantu možného řešení: On-premise: dodávka a implementace HW a SW v místě Objednatele s níže uvedenou podporou na správu dodaného řešení:

* Pokud se řešení skládá z více modulů, musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jednou, centrální správou na jednom hardware
* Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz, pro neomezený počet uživatelů a SSL VPN tunelů pro vzdálené připojení uživatelů
* Všechny služby musí být poskytovány jedním zařízením typu hardware appliance
* Řešení musí mít funkcionalitu vysoké dostupnosti (active-passive) pro všechny prvky poskytující funkce uvedené v bodu 2, s výjimkou logování, karantény a rozšířeného reportování, a to bez dalších licenčních nákladů (přípustné jsou pouze náklady na hardware)
* Dodavatel provede analýzu funkčností stávajícího Firewall clusteru (Juniper SRX240) a navrhne optimální nastavení funkčností a přenesení pravidel do nového řešení
* Dodavatel provede test funkčnosti dodaného řešení před ostrým spuštěním

## Požadované funkce a vlastnosti

## Paketový filtr a základní funkce

|  |  |
| --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | **Dodavatel vyplní ANO, pokud požadavek splní, NE pokud nesplní** |
| Stavové filtrování paketů |  |
| Překlady komunikace (příchozí i odchozí) |  |
| Možnost použití více internetů v režimu active-backup nebo balancing (dynamické routování). |  |
| Montáž do standardních 19" skříní (rack). |  |
| 100% administrace pouze přes webové rozhraní (bez nutnosti použít textové rozhraní typu telnet/ ssh konzole) |  |
| Propojení a využívání Active Directory |  |
| Podpora bezagentového přihlášení uživatelů (8. vrstva) |  |
| DHCP server a DNS forwarder pro konkrétní sítě |  |
| Možnost automatické zálohy UTM a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy |  |
| Šifrování záloh |  |
| Logování a rozšířený reporting (vč. statistik uživatelských aktivit) |  |
| Podpora vrácení se na předchozí verzi software (po aktualizaci) |  |
| Vlastní API rozhraní pro propojení s dalšími interními nástroji |  |
| Podpora routování BGP a OSPF |  |

## Proaktivní ochrana perimetru

|  |  |
| --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | **Dodavatel vyplní ANO, pokud požadavek splní, NE pokud nesplní** |
| IDS/IPS |  |
| Blokování C&C komunikace |  |
| Možnost specifikace výjimek |  |
| Identifikování kompromitovaného systému na základě C&C komunikace (stačí IP adresa) |  |
| Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce) |  |
| Logování |  |

## VPN – vzdálené přístupy

|  |  |
| --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | **Dodavatel vyplní ANO, pokud požadavek splní, NE pokud nesplní** |
| IPSEC – propojení vzdálených lokalit, včetně podpory IKEv2 |  |
| SSL VPN – připojení vzdálených PC |  |
| SSL VPN - Odlišný certifikát / uživatel |  |
| SSL VPN - Uživatelský portál pro stažení VPN klienta |  |
| SSL VPN - Dostupná instalace vč. konfigurace (bez nutnosti další konfigurace na koncových počítačích) |  |
| Zobrazení aktuálně připojených uživatelů v GUI |  |
| Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat |  |
| Neomezený počet SSL VPN klientů v ceně |  |
| Logování |  |

## Reverzní proxy pro ochranu interních webových serverů a aplikací

|  |  |
| --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | **Dodavatel vyplní ANO, pokud požadavek splní, NE pokud nesplní** |
| Ochrana skenováním antimalware motorem |  |
| Filtrování http a https komunikace |  |
| Ochrana proti trojským koním |  |
| Ochrana proti podvržení cookies (podepisování) |  |
| Možnost monitorovat nebo blokovat (odmítnout) komunikaci |  |
| Podpora vytváření přihlašovacích formulářů navázaných na Active Directory |  |
| Blokování komunikace na základě reputační služby výrobce |  |
| Blokování útoků typu SQL injection |  |
| Možnost specifikace výjimek |  |
| Logování |  |

## Ochrana emailové komunikace (SMTP)

|  |  |
| --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | **Dodavatel vyplní ANO, pokud požadavek splní, NE pokud nesplní** |
| Ochrana skenováním antimalware motorem |  |
| Ochrana proti spamům / phishing emailům |  |
| Skenování příloh emailů vč. archivů |  |
| Skenování odchozího i příchozího provozu |  |
| Blokování komunikace na základě reputační služby výrobce |  |
| Ochrana proti DoS útokům |  |
| Nastavitelná a vynutitelná TLS komunikace pro konkrétní SMTP servery |  |
| Volitelný TLS certifikát pro interní MTA |  |
| Šifrování odchozích emailů (nastavitelné a volitelné) |  |
| Kontrola emailové fronty ze stejného webového rozhraní |  |
| Emailová karanténa uložená přímo na zařízení |  |
| Logování a prohledávání logů min. na úrovni: Odesílatel, Příjemce, Předmět |  |
| Náhled uživatele do karantény pomocí GUI „uživatelského portálu“ (jen pro emaily konkrétního uživatele) a možnost uvolnění spamů |  |
| Greylisting |  |
| Blokace na základě SPF a RBL |  |
| Blokace příloh dle typu souborů na základě MIME hlaviček |  |
| Ověření adresy příjemce z emailového serveru na úrovni SMTP dotazu |  |
| Sandboxing |  |
| Možnost specifikace výjimek |  |
| Logování |  |

## Ochranu přístupů na internet

|  |  |
| --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | **Dodavatel vyplní ANO, pokud požadavek splní, NE pokud nesplní** |
| Ochrana skenováním antimalware motorem |  |
| URL filtrování (min. 80+ kategorií) |  |
| Filtrování HTTP, HTTPS a FTP |  |
| Možnost specifikovat povolené porty |  |
| Možnost specifikace porty proxy |  |
| Propojení s Active Directory |  |
| Možnost definovat výjimky |  |
| Pravidla lze uplatnit pouze ve specifikovaný čas během dne |  |
| Pravidla lze specifikovat na skupinu/uživatele z Active Directory |  |
| Sandboxing |  |
| Logování |  |

## Možnost rozšíření o správu WiFi

Řešení musí být rozšiřitelné o správu wifi zařízení (vše od stejného výrobce) a nesmí k tomu vyžadovat žádnou další licenci.

## Připojení vzdálených poboček

Řešení musí mít možnost připojit vzdálené pobočky přes internet a vlastním radiovým spojem pomocí šifrovaného VPN tunelu a dalších zařízení na druhé straně. VPN tunel musí běžet na 2. vrstvě a cílová zařízení v koncové lokalitě nesmí vyžadovat žádnou další licenci. Součástí dodávky musí být řešení s vysokou dostupnosti pro pracoviště Orlová a řešení bez požadavku na vysokou dostupnost pro pracoviště Mizerov. Dodaná zařízení musí být od stejného výrobce jako primární řešení. Požadované rychlostí připojení do jednotlivých lokalit (pracovišť):

Lokalita Orlová: 100 MB přes Internet + 100 MB přes vlastní radiový spoj

Lokalita Mizerov: 40 MB přes vlastní radiový spoj

## Minimální technické požadavky (propustnosti deklarované výrobcem)

**Lokalita Karviná**

* Maximální počet uživatelů: neomezeno
* Firewall: >25 Gbps
* Firewall IMIX: >7 Gbps
* IPS propustnost: >5 Gbps
* VPN propustnost: >2,5 Gbps
* Propustnost Web proxy s aktivním AV: >3 Gbps
* Souběžná spojení: >15 miliónů
* Nová spojení za sekundu: >100 tisíc

**Lokalita Orlová**

* VPN propustnost: >1 Gbps
* Souběžná spojení: >8 miliónů
* Nová spojení za sekundu: >100 tisíc

**Lokalita Mizerov**

* VPN propustnost: >40 Mbps