***Příloha č. 1 Kupní smlouvy Specifikace předmětu plnění***

# Obecné požadavky

Předmětem plnění této zakázky je návrh, dodávka, instalace, zprovoznění, dokumentace skutečného provedení, zaškolení administrátorů a podpora provozu nového firewallu.

Firewall musí být odolný proti výpadku jakékoliv jeho části i celé jedné poloviny bez dopadu na provoz aplikací a dostupnost dat.

Firewall bude umístěn v LAN síti Dopravního podniku Ostrava a. s.. Návrh a nabízená konfigurace musí umožňovat výhledové umístění ve dvou technických místnostech vzdálených max. 15km a to bez jakýchkoliv dalších investic, kromě výměny potřebné optické kabeláže propojující technické místnosti.

Dodavatel je povinen v rámci plnění veřejné zakázky garantovat nabízené technické parametry a doložit přesné označení nabízeného produktu včetně jeho technických parametrů pro ověření splnění požadavků Zadavatele.

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). Zboží musí být určeno pro český trh. Zadavatel požaduje potvrzení výrobce, že se jedná o zboží pro český trh. Zadavatel bude v DB výrobce uveden jako první vlastník.

Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení), že jsou určeny pro český trh.

# Požadované technické parametry zařízení

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Požadovaná funkcionalita/vlastnost** | **Splňuje ANO/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| **HW a SW parametry** | 2ks Next Generation Firewallů zapojených do clusteru – dále jen FW. |  |  |
|  | 1ks zařízení pro připojení vzdálené pobočky |  |  |
| FW musí být typu HW appliance. |  |  |
| FW musí být rozměrově kompatibilní s 19" skříní (rack). |  |  |
| Každý nód clusteru musí obsahovat minimálně 4 SFP+ datové porty (včetně transceiverů) o rychlosti 10Gbps s možností vytvářet na nich subinterfaces a těm přidělovat různé VLANy a další IP adresy. |  |  |
| FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP). |  |  |
| Možnost zálohy konfigurace FW a v případě potřeby kompletní obnova konfigurace nahráním ze zálohy. |  |  |
| Pokud se FW skládá z více modulů, musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jednou, centrální správou. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW (délky platnosti licence). |  |  |
| Nabízený FW musí být nejnovější model výrobce a nesmí mít ohlášeno datum o ukončení výroby či podpory tzn. staré modely budou ze soutěže vyřazeny. |  |  |
| Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz, pro neomezený počet uživatelů a nezávislý na počtu ochraňovaných koncových systémů, nebo počtu používaných internetových doménových jmen. |  |  |
| Řešení musí mít funkcionalitu vysoké dostupnosti pro všechny prvky poskytující požadované funkce, s výjimkou logování a rozšířeného reportování, a to bez dalších licenčních nákladů (přípustné jsou pouze náklady na hardware). |  |  |
| Požadované funkcionality – Firewall, Identity Aware, Application Control, URL filtering, IPS, IPSec VPN, SSL Remote Access, Antivirus, Anti-Spyware, Clustering, cloudový Sandboxing. |  |  |
|  Každý firewall bude mít 2ks napájecích zdrojů |  |  |
| **Požadavky na High Availability (HA) FW** | FW musí používat režim HA v módu Active-Passive složený alespoň ze dvou zařízení. |  |  |
|  | Veškeré informace o probíhajícím provozu musí být synchronizovány tak, aby při výpadku jednoho z boxů nedošlo k nežádoucí ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP a UDP procházejícího přes FW. |  |  |
| FW musí být schopen provést failover na základě stavu jednoho ze síťových interface (up/down) nebo nedostupnosti IP adresy druhého FW v HA. |  |  |
| **Obecné minimální výkonové parametry FW (deklarovány výrobcem** | Propustnost FW při zapnutí všech dostupných ochran (plné aplikační kontrole, IPS, Antivirus, URL filteringu, Anti-Spyware, Sandboxingu) a zapnutí logování musí dosahovat hodnoty alespoň 2,5Gbps (Threat prevention troughput). |  |  |
|  | Propustnost NGFW a zapnutí logování musí dosahovat hodnoty alespoň 5Gbps. |  |  |
| Minimální počet souběžných spojení - 990 000 |  |  |
| Minimální počet nových spojení za sekundu – 53000 |  |  |
| **Síťová funkcionalita FW** | FW musí plně podporovat IPv4 i IPv6 |  |  |
|  | FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64 |  |  |
| Možnost použití více internetových připojení v režimu active-backup nebo balancing (ECMP - Equal Cost Multiple Path). |  |  |
| DHCP server a DHCP relay pro konkrétní sítě |  |  |
| FW musí podporovat minimálně 20 oddělených bezpečnostních zón, mezi nimiž je možno nastavovat pravidla pro prostupy mezi zónami. |  |  |
| FW musí podporovat směrování typu Static route, RIP, OSPF, BGP a na základě politiky (Policy Based Forwarding) |  |  |
| PBF musí být možno nakonfigurovat na základě dostupných metrik typu interface, IP adresa, zóna, uživatel. |  |  |
| **VPN:** | FW musí mít licenčně neomezený počet site-to-site VPN pomocí protokolu IPSec |  |  |
|  | FW musí podporovat Remote Acess VPN pomocí protokolů IPSec a TLS |  |  |
| FW musí podporovat Clientless Remote Access VPN |  |  |
| Počet současně připojených uživatelů musí být alespoň 1000 |  |  |
| Propustnost IPSec musí být alespoň 2Gbps. |  |  |
| **Vzdálené lokality – dočasné záložní připojení** | 1ks zařízení pro bezpečné připojení vzdálené lokality přes VPN na 2. vrstvě (např. L2TP/IPSec) |  |  |
|  | Použije se především při výpadku primární konektivity vzdálené lokality |  |  |
| Zařízení musí být možno přenést na kteroukoli lokalitu, a připojit tunel přes LTE nebo ethernet. |  |  |
| Připojení musí umožnit přenos VLAN tagů (minimálně 4 VLANy) |  |  |
| **Management FW** | Jednotlivé HW appliance musí obsahovat grafické rozhraní (GUI) pro správu, bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování |  |  |
|  | FW musí obsahovat nativní nástroj pro odchycení provozu |  |  |
| FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem |  |  |
| Out-of-band management port |  |  |
| **Aplikační kontrola** | FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu |  |  |
|  | Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla |  |  |
| FW musí podporovat identifikaci aplikací na nestandardních portech |  |  |
| FW musí podporovat identifikaci aplikace napříč všemi porty/protokoly |  |  |
| Identifikace aplikace musí probíhat přímo ve FW |  |  |
| **Kontrola na úrovni uživatelských identit** | FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit |  |  |
|  | Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla |  |  |
| FW musí podporovat získávání vazby IP adresa – uživatelské jméno bez nutnosti instalace klienta na koncové zařízení. |  |  |
| FW musí podporovat vázání bezpečnostních filtrů (IPS, Webová kategorie, Antivirus, Sandboxing) na základě uživatelské identity (uživatel nebo skupina v Active Directory) a toto musí být nativní součástí vytváření standardního bezpečnostního pravidla. |  |  |
| Na základě chování uživatelů, především pak surfování na internetu a C&C komunikace, musí být FW schopen vygenerovat hodnocení uživatelů a upozornit na nebezpečné uživatele. |  |  |
| FW musí podporovat získávání vazby IP adresa – uživatelské jméno z Active Directory za pomoci doménového účtu s co nejmenšími možnými právy pro čtení security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins) |  |  |
| **Dekrypce** | FW musí podporovat dekrypci odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům |  |  |
|  | FW musí podporovat dekrypci příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru |  |  |
| FW musí podporovat funkci SSH proxy a kontrolovat tunelované aplikace |  |  |
| Dekryptovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita |  |  |
| FW musí podporovat dekrypci za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz |  |  |
| FW musí podporovat přeposílání dešifrovaného provozu pro potřeby archivace provozu. |  |  |
| **Cloudový Sandboxing** | Sandboxing systém musí být od stejného výrobce, jako je FW |  |  |
|  | Sandboxing nesmí vyžadovat žádné další HW zařízení nebo správu mimo FW |  |  |
| Sandboxing systém musí být schopen analyzovat podezřelé soubory, a to jak přílohy v SMTP, IMAP a POP3 komunikaci, tak soubory v HTTP(S) a SMB komunikaci. |  |  |
| Sandboxing systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro FW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý |  |  |
| Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android |  |  |
| Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní FW |  |  |
| Aktualizace zero-day signatur musí být instalována do FW v intervalu max. 5 minut. |  |  |
| **Bezpečnostní funkcionality** | FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu –povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu |  |  |
|  | FW musí obsahovat integrovaný systém ochrany proti zranitelnostem a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla |  |  |
| FW musí obsahovat antivirový engine pro skenování provozu v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB |  |  |
| FW musí podporovat možnost zablokování komunikace se známými C&C servery i v případě, že je provoz šifrován a není možné provádět SSL dekrypci |  |  |
| FW musí v takovém případě jednoznačně identifikovat původce C&C komunikace |  |  |
| FW musí, pro přístup ke kritickým aplikacím, poskytovat možnost vynutit více faktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje více faktorovou autentizaci. |  |  |
| FW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu |  |  |
| FW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru |  |  |
| Zablokování útoků typu Cross Site (XSS) a SQL injection útokům |  |  |
| IP Geolocation Policy pro možnost povolení nebo zablokování přístupu z jednotlivých států |  |  |
| Výrobce FW se musí nacházet v kvadrantu „Leaders“ Enterprise Network Firewalls reportu společnosti Gartner v posledním aktuálním reportu |  |  |
| **URL filtering** | FW musí obsahovat nativní podporu pro využívání databáze URL tak, aby bylo možno zakázat určité kategorie URL (například Games, Gambling, Hacking, Sex, …) |  |  |
|  | FW musí podporovat vytváření administrátorsky definovaných kategorií, Allowlist, Blocklist |  |  |
| URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL vedoucích na škodlivý obsah, nebo C&C centra |  |  |
| URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL |  |  |
| **Logování** | FW musí obsahovat logování (lokálně, a na logserver) a rozšířený reporting (vč. statistik uživatelských aktivit) |  |  |
|  | FW musí obsahovat nástroj pro analýzu logů (zpětný náhled do logů) bez nutnosti využití dalšího systému mimo GUI |  |  |
| **Záruka, servis a služby** | Záruka min. 5 let se servisem v místě instalace s reakcí minimálně NBD (NextBusinessDay) |  |  |
|  | Záruka garantovaná výrobcem |  |  |
| SW podpora výrobce minimálně 5 let |  |  |
| Instalace, konfigurace a integrace |  |  |
| Zaškolení obsluhy |  |  |