Příloha č. 6

**Technická specifikace – firewall Fortinet (4 ks)**

**Obecné požadavky**

* 4x hardware appliance (2 lokality, každá po dvou boxech) s podporou výrobce v režimu 24x7 a aktualizací všech požadovaných bezpečnostních funkcí po dobu 1 roku pro použití v režimu vysoké dostupnosti (active-active, active-passive)
* velikost 1 RU
* Podpora virtualizace uvnitř HW appliance formou vytváření virtuálních kontextů
* Grafické konfigurační rozhraní a příkazový řádek
* Minimální počty požadovaných síťových rozhraní:

o 12x GE RJ 45

o 2x 10GE SFP+

o Konzole sériové linky pro přístup k příkazovému řádku

* Podpora plnohodnotné inspekce sítového provozu v režimech

o NAT/router

o L2 transparentní režim (dva a více sítových rozhraní)

o L2 interface pair (dvě sítové rozhraní)

**Výkonové požadavky**

Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání.

* Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 18 Gbps (UDP pakety o velikosti 512 B)
* Nízké vložené zpoždění zařízení (latence) max 5μs
* Minimální počet současně navázaných spojení firewallu 1.5 M
* Minimální počet nových spojení za sekundu 56 k
* Výkon zařízení min. 15 M paketů / sekundu
* Propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)

o Propustnost IPS ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 2,6 Gbps

o Propustnost NGFW (kombinace stavového firewallu, IPS, rozpoznávání aplikací na L7, logování) min. 1,6 Gbps

o Propustnost TP ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 1 Gbps

* Propustnost IPsec VPN v konfiguraci AES256/SHA256 min. 11,5 Gbps
* Propustnost funkce SSL inspekce provozu min. 1 Gbps
* Min. počet konfigurovatelných virtuálních kontextů na každém zařízení 10

**Funkční požadavky**

* Podpora a zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) minimálně s ohledem na tyto bezpečnostní funkce:
* Funkce rozpoznávání kancelářských a průmyslových aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací a 700 průmyslových aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací
* Funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min. 10 000 signatur v databázi; podpora zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT)
* Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předání zkoumaných souborů pro analýzu v prostředí typu sandbox
* Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze.
* Detekce úniku dat
* Funkce SSL inspekce pro kontrolu protokolů s možností vytváření protokolů výjimek. Výjimky z SSL inspekce požadujeme minimálně:
* na základě administrátorem definovaných adres
* na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.)
* Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
* Možnost nastavovat firewall politiku na základě geografických údajů
* Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace
* Detekce klientského zařízení, možnost nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, …) bez nutnosti instalovat klienty na koncové stanice
* Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky
* Funkce QoS, traffic shaping
* Funkce klientské VPN (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál, možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů
* site-to-site IPsec VPN s podporou statického i dynamického routování
* Podpora OT/ICS/IoT protokolů (minimálně klasifikace provozu, identifikace zařízení, ochrana zařízení před sítovým útokem)
* Umístění výrobce v Gartner MQ for Network Firewalls v sekci „Leaders“ v posledních 3 letech