Krajská zdravotní nemocnice Ústeckého kraje

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
tel.: +420 477 111 111
fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Příloha č. X Technická specifikace

k veřejné zakázce s názvem „**Pořízeni řešení firewallu včetně VPN agregátoru řešení pro KZ jednodenní chirurgie a ambulance, s.r.o.“**

Předmětem veřejné zakázky je nákup jednoho kusu UTM firewall. Zařízení musí po dodání splňovat funkčnost, technické parametry a ostatní požadavky dle zadání viz body 1-4. Součástí dodávky musí být instalaci zařízení. Implementace nesmí ohrozit, ani omezit, stávající provoz infrastruktury zadavatele, ani jeho dceřiné společnosti.

1. Požadavky na nové FW zařízení:

HW požadavky:

- HW appliance (VM appliance ani software řešení není akceptovatelné)
- Velikost 1 RU
- Duální napájení (redundantní zdroje) součástí dodávky
- Minimálně 2 x 10 GbE SFP+ síťová rozhraní
- Minimálně 2 x 10 GbE SFP+ síťová rozhraní pro HA rozhraní
- Minimálně 8x 1 GbE SFP síťová rozhraní
- Minimálně 16x 1 GbE RJ45 síťová rozhraní
- Management rozhraní 1 GbE RJ45
- Sériový konzolový port v provedení portu RJ45.
- Lokální uložiště instalované přímo ve FW zařízení. Toto uložiště musí být bez pohyblivých částí a s kapacitou alespoň 1 x 480 GB.

Funkční požadavky:

- Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů
- Bezpečnostní funkce obecně označovaných jako Next Generation firewall
- Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení, kdy každý virtuální kontext musí pracovat izolovaně
- Podpora stavového firewallu pro IPv4 i IPv6, podpora nat 64/46
- Možnost volby funkce v režimu NAT/router i L2 (bridge) včetně koexistence různých režimů na jednom zařízení pomocí podporované virtualizace

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
tel.: +420 477 111 111
fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

- Výrobcem deklarovaná a garantovaná nízká vložená latence firewallu se všemi zapnutými funkcemi (max. v řádu do deseti mikrosekund (µs)
- Plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall plnohodnotně konfigurovat i ve chvílí, kdy z jakéhokoliv důvodu centrální správa nebude dostupná)
- Ověřování identity uživatelů (napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On
- Integrovaná funkce explicitní proxy s podporou http, https, socks včetně autentizace uživatelů a všech bezpečnostních funkcí
- Funkce QoS, traffic shaping, SD-WAN
- Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup.
- VPN klient pro neomezený počet přistupujících zařízení součástí nabídky
- Podpora funkce SSL inspekce (MITM), včetně podpory minimálně TLS 1.3
- Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce (viz dále) včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.
- Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 3000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace
- 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, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu
- Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
tel.: +420 477 111 111
fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

- Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě watermarků, popisu regulárním výrazem atp.
- Podpora dvoufaktorové autentizace pomocí mobilních OTP tokenů, součástí nabídky musí být licence pro mobilní OTP tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN, dvoufaktorová autentizace (pomoc s konfigurací klientů u koncových uživatelů, dodání netechnického popisu konfigurace pro uživatele s BYOD zařízeními pro systémy Windows, MacOS)
- Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného firewallu s dalšími poptávanými nebo již instalovanými bezpečnostní prvky (mailová brána, sandbox).

Výkonové požadavky:

- Počet současně navázaných spojení firewallu min. 2 900 000 počet nových spojení za sekundu min. 270 000

  s podporu všech zapnutých inspekčních mechanizmy
- Celková propustnost IPSEC VPN při použití AES256-SHA256 min. 12,7 Gbps
- Propustnost SSL VPN min. 1,9 Gbps
- Min. počet současně připojených uživatelů SSL VPN 500
- Min. počet současně připojených IPSEC Gateway-to-gateway VPN 2000
- Min. počet současně připojených IPSEC Client-to-gateway VPN 15000
- Propustnost funkce SSL inspekce min 10 Gbps
- Propustnost funkce IPS min. 3.7 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)
- Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 3,5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
- Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 2,9 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
- Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
tel.: +420 477 111 111
fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Licenční požadavky:

- Součástí dodávky musí licence s nárokem na SW podporu (kladení dotazů, pomoc s řešením konfiguračních problémů, hlášení chyb v českém jazyce) v režimu 24x7 a hardwarová podpora rozsahu 5/8 s výměnou hardware do následujícího pracovního dne a to na minimálně 1 roky s udržitelností po dobu minimálně 5 let.

- Součástí dodávky musí být licence zaručující přístup pro miminálně 250 SSL VPN klientů přes 2 faktorové ověření (a to ve formě 250 licencí na produkt Cisco DUO jež rozšíří stávající licence zadavatele na dobu 3 let)
- Bezpečnostní funkce musí být dodány minimálně v rozsahu IPS, Antivirus, Virus Outbreak protection, ochrana před Malware a Antispam proteochrana. Dále pak licence dovoluje filtraci obsahu webových stránek a video obsahu. Vše na minimálně na 1 rok s udržitelností po dobu minimálně 5 let.

3. Implementace

- Rozsah Implementace:
  - ▪ Spuštění zařízení do provozu
  - ▪ Zapojení do sítě KZ
  - ▪ Nastavení managementu
  - ▪ Vytvoření 2 firewallových kontextů
  - ▪ Implementace dvoufaktorové autentizace pro SSL-VPN uživatele, dodání netechnického postupu konfigurace klienta pro předání uživatelům, pomoc s případnými implementačními obtížemi.
  - ▪ zaškolení obsluhy zadavatele
  - ▪ Vypracování akceptačních testů na základě asistované implementace

4. Obchodní podmínky

· Všechny dodané komponenty musí být nové a nepoužité, přičemž se na ně musí vztahovat minimálně záruka vycházející z formy podpory a uplatňovaná v autorizovaném servisním středisku v České republice

· Požadujeme referenci v ČR na nabízené zboží a poptávanou funkcionalitu

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
tel.: +420 477 111 111
fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Při nesplnění akceptačních a obchodních podmínek si objednatel vyhrazuje zboží nepřevzít.

Požadavky na předmět plnění uvedené v tomto dokumentu jsou závazné, jejich nedodržení bude považováno za nesplnění zadávacích podmínek s následkem vyloučení dodavatele z účasti v zadávacím řízení.

Dodavatel prohlašuje, že jím nabízené plnění splňuje všechny požadavky uvedené v této Příloze č. x Technická specifikace:

V ……(vyplní účastník)…… dne …(vyplní účastník)…

Za společnost

……(vyplní účastník)……

Osoba oprávněná jednat jménem či za účastníka (pozice, titul, jméno, příjmení)

……(vyplní účastník)…….