**Příloha č. 2 zad. dokumentace**

**Technické specifikace předmětu plnění**

Nabízené zboží a materiál musí být nové a nepoužité, licencované jménem zadavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.

Účastník je povinen s dodávkou doložit oficiální potvrzení výrobce o určení dodávaného HW (seznam sériových čísel) pro český trh a koncové zákazníky Zdravotnický holding Královéhradeckého kraje a.s., Oblastní nemocnici Náchod a.s., Oblastní nemocnici Jičín a.s., Oblastní nemocnici Trutnov a.s., Městskou nemocnici, a.s., pokud o to zadavatel požádá.

Celá dodávka musí obsahovat všechny HW a SW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. Veškeré poptávané podpory jsou v režimu 7x24.

Součástí dodávky je výměna stávajících firewallů za nové a zprovoznění dodávaného řešení. Cena za tuto službu bude uvedena jako součást ceny poptávaného řešení. Ceny uvede uchazeč do cenové kalkulace, která tvoří přílohu č.6 ZD.

1. **Požadujeme dodání řešení typu Next Generation FireWall (NGFW) v HA zapojení (2 ks HW boxů) dle níže uvedené specifikace.**

**Základní technické požadavky**

* HW appliance NGFW/UTM firewallu
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU
* Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu
* Požadujeme možnost doplnit druhý napájecí zdroj (interní nebo externí).
* Min. 2x 10 GE SFP+ rozhraní firewallu využitelných pro zpracování komunikace
* Min. 8x 1 GE RJ45 rozhraní firewallu využitelných pro zpracování komunikace
* Min. 8x 1 GE SFP rozhraní firewallu využitelných pro zpracování komunikace
* 2 x samostatné 1GE rozhraní pro management
* konzolový port pro management
* Podpora režimu vysoké dostupnost (režim L2 cluster, tedy využití virtuálních MAC adres; celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-active (A/A) a active-passive (A/P). Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky.

**Požadované síťové a bezpečnostní funkce**

**Součástí dodávky musí být i příslušná licence (je-li výrobcem požadována) na 5 let. Požadované výkonnostní parametry musí být oficiálně deklarovány výrobcem firewallu.**

* Podpora VLAN, min. 1.000
* Podpora LACP
* Počet FW pravidel min. 5.000
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace nikoliv pouhý TCP/UDP port).
* Celková propustnost firewall min. 20 Gbps (měřeno na UDP paketech o velikosti 64B)
* Vložená latence firewallu nepřesahuje 3 µs (měřeno na malých UDP paketech (64B))
* Počet nově navázaných TCP spojení (setup-rate) min. 250.000 za sekundu
* Celkový počet konkuretních TCP spojení firewallu 6 milionů

**Funkce detekce aplikací na L7 (Application Control)**

* Detekce známých aplikací na základě signatur
* Signaturové databáze automaticky aktualizované výrobcem
* Alespoň 3.000 podporovaných aplikací
* Pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)
* Možnost tvorby vlastních signatur
* Detekované aplikace je možné: povolit, monitorovat, blokovat
* Na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
* Propustnost funkce Application Control včetně logování minimálně 12 Gbps
* Funkce Application Control se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.

**Funkce detekce a potlačení narušení (IPS/IDS)**

* Signatury automaticky aktualizované výrobcem
* Alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
* Možnost tvorby vlastních signatur
* Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
* Propustnost funkce IPS včetně logování min. 7,5 Gbps (měřeno na komunikaci typu mix aplikací)

**Funkce antivirové kontroly**

* Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem
* Signatury automaticky aktualizované výrobcem
* Požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
* Možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce
* Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 4,5 Gbps
* Funkce AV kontroly se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
* Podpora služby výrobce, která umožní detekovat malware, který byl objeven v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
* Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu v reálném čase odstraní aktivní obsah z dokumentu. Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky a je doručen příjemci. Originální dokument je odeslán ke kontrole do Sandboxu.
* Podpora SSL dekrypce/SSL inspekce s minimální propustností 5,5 Gbps (TLS 1.2AES 256-SHA, měřeno v kombinaci s IPS kontrolou)

**Funkce IPSEC VPN**

* Podpora site-to-site VPN
* Podpora klientských VPN
* Dostupnost VPN klienta pro koncové stanice (Windows, MacOS)
* Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů, v opačném případě požadujeme dodání neomezené licence.
* Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1.000
* Propustnost IPSec VPN min. 20 Gbps (měřeno při AES 256)
* Podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
* Podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování

**Funkce SSL VPN**

* Podpora klientského i bezklientského (portálového) režimu
* Minimální počet současně navázaných SSL VPN tunelů: 5000
* Minimální propustnost SSL VPN: 4,5 Gbps

**Funkce kategorizace webových stránek**

* Založená na centrálně spravované databázi výrobce
* Minimálně 50 filtračních kategorií
* Možnost definice vlastních kategorií
* Možnost definice vlastních seznamů zakázaných URL
* Kategorizace musí zahrnovat i české a slovenské internetové stránky

**Funkce DNS filtru**

* Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u kategorizace webových stránek)
* Možnost definovat vlastní tzv. blacklist domén
* Možnost přesměrovat komunikace se zakázanými doménami na vlastní portál/URL

**Funkce ochrany před únikem citlivých informací (DLP)**

* Možnost analýzy běžných typů dokumentů a protokolů
* Možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum

**Podpora funkce explicit proxy**

* Podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
* Funkce transparentního ověřování uživatelů pomocí domény MS Active Directory včetně podpory autentizace uživatelů na terminálovém serveru

**Virtualizace**

* Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné FW řešení včetně odděleného GUI, managementu účtů, atp.
* Součástí dodávky musí být licence na min. 5 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
* Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)

**Management**

* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

**Certifikace**

* Certifikace ICSA Labs minimálně pro Firewall, IPSec VPN, IPS, Antivirus, SSL VPN

1. **Požadujeme dodání řešení typu Next Generation FireWall (NGFW) 5 ks od stejného výrobce jako řešení dodané v bodu A) se stejným operačním systémem. Z toho 1 kus bude pouze box s HW podporou na 5 let v režimu 7x24 a 4 kusy budou včetně všech dalších požadovaných síťových a bezpečnostních funkcionalit dle níže uvedené specifikace.**

**Základní technické požadavky**

* HW appliance NGFW/UTM firewallu
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU
* Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu
* Požadujeme možnost doplnit druhý napájecí zdroj (interní nebo externí).
* Min. 2x 10 GE SFP+ rozhraní firewallu využitelných pro zpracování komunikace
* Min. 16x 1 GE RJ45 rozhraní firewallu využitelných pro zpracování komunikace
* Min. 8x 1 GE SFP rozhraní firewallu využitelných pro zpracování komunikace
* 2 x samostatné 1GE rozhraní pro management
* konzolový port pro management
* Podpora režimu vysoké dostupnost (režim L2 cluster, tedy využití virtuálních MAC adres; celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-active (A/A) a active-passive (A/P). Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky.

**Požadované síťové a bezpečnostní funkce**

**Součástí dodávky musí být i příslušná licence (je-li výrobcem požadována) na 5 let. Požadované výkonnostní parametry musí být oficiálně deklarovány výrobcem firewallu.**

* Podpora VLAN, min. 1.000
* Podpora LACP
* Počet FW pravidel min. 5.000
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace nikoliv pouhý TCP/UDP port).
* Celková propustnost firewall min. 8 Gbps (měřeno na UDP paketech o velikosti 64B)
* Vložená latence firewallu nepřesahuje 5 µs (měřeno na malých UDP paketech (64B))
* Počet nově navázaných TCP spojení (setup-rate) min. 50.000 za sekundu
* Celkový počet konkuretních TCP spojení firewallu 1 milion

**Funkce detekce aplikací na L7 (Application Control)**

* Detekce známých aplikací na základě signatur
* Signaturové databáze automaticky aktualizované výrobcem
* Alespoň 3.000 podporovaných aplikací
* Pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)
* Možnost tvorby vlastních signatur
* Detekované aplikace je možné: povolit, monitorovat, blokovat
* Na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
* Propustnost funkce Application Control včetně logování minimálně 2 Gbps
* Funkce Application Control se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.

**Funkce detekce a potlačení narušení (IPS/IDS)**

* Signatury automaticky aktualizované výrobcem
* Alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
* Možnost tvorby vlastních signatur
* Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
* Propustnost funkce IPS včetně logování min. 1,5 Gbps (měřeno na komunikaci typu mix aplikací)

**Funkce antivirové kontroly**

* Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem
* Signatury automaticky aktualizované výrobcem
* Požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
* Možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce
* Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 0,6 Gbps
* Funkce AV kontroly se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
* Podpora služby výrobce, která umožní detekovat malware, který byl objeven v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
* Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu v reálném čase odstraní aktivní obsah z dokumentu. Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky a je doručen příjemci. Originální dokument je odeslán ke kontrole do Sandboxu.
* Podpora SSL dekrypce/SSL inspekce s minimální propustností 0,8 Gbps (TLS 1.2AES 256-SHA, měřeno v kombinaci s IPS kontrolou)

**Funkce IPSEC VPN**

* Podpora site-to-site VPN
* Podpora klientských VPN
* Dostupnost VPN klienta pro koncové stanice (Windows, MacOS)
* Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů, v opačném případě požadujeme dodání neomezené licence.
* Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1.000
* Propustnost IPSec VPN min. 9 Gbps (měřeno při AES 256)
* Podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
* Podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování

**Funkce SSL VPN**

* Podpora klientského i bezklientského (portálového) režimu
* Minimální počet současně navázaných SSL VPN tunelů: 250
* Minimální propustnost SSL VPN: 0,6 Gbps

**Funkce kategorizace webových stránek**

* Založená na centrálně spravované databázi výrobce
* Minimálně 50 filtračních kategorií
* Možnost definice vlastních kategorií
* Možnost definice vlastních seznamů zakázaných URL
* Kategorizace musí zahrnovat i české a slovenské internetové stránky

**Funkce DNS filtru**

* Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u kategorizace webových stránek)
* Možnost definovat vlastní tzv. blacklist domén
* Možnost přesměrovat komunikace se zakázanými doménami na vlastní portál/URL

**Funkce ochrany před únikem citlivých informací (DLP)**

* Možnost analýzy běžných typů dokumentů a protokolů
* Možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum

**Podpora funkce explicit proxy**

* Podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
* Funkce transparentního ověřování uživatelů pomocí domény MS Active Directory včetně podpory autentizace uživatelů na terminálovém serveru

**Virtualizace**

* Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné FW řešení včetně odděleného GUI, managementu účtů, atp.
* Součástí dodávky musí být licence na min. 5 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
* Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)

**Management**

* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

**Certifikace**

* Certifikace ICSA Labs minimálně pro Firewall, IPSec VPN, IPS, Antivirus, SSL VPN

1. **Požadujeme dodání 5 ks řešení typu Next Generation FireWall (NGFW) stejného výrobce jako řešení dodané v bodu A) se stejným operačním systémem. Z toho 3 kusy budou pouze boxy s HW podporou na 5 let v režimu 7x24 a 2 kusy budou včetně všech dalších požadovaných síťových a bezpečnostních funkcionalit dle níže uvedené specifikace.**

**Základní technické požadavky**

* HW appliance NGFW/UTM firewallu
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU, nebo s umístěním na polici
* Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu
* Min. 8x 1 GE RJ45 rozhraní firewallu využitelných pro zpracování komunikace
* konzolový port pro management

**Požadované síťové a bezpečnostní funkce.**

**Součástí dodávky musí být i příslušná licence (je-li výrobcem požadována) na 5 let. Požadované výkonnostní parametry musí být oficiálně deklarovány výrobcem firewallu.**

* Všechny funkcionality (kromě výkonnostních) shodné jako pro řešení specifikované v bodě A)

**Minimální výkonnostní parametry**

* Celková propustnost firewall min. 3 Gbps (měřeno na UDP paketech o velikosti 64B)
* Vložená latence firewallu nepřesahuje 5 µs (měřeno na malých UDP paketech (64B))
* Počet nově navázaných TCP spojení (setup-rate) min. 20.000 za sekundu
* Celkový počet konkuretních TCP spojení firewallu 1 milion
* Propustnost funkce Application Control včetně logování minimálně 0,6 Gbps
* Propustnost funkce IPS včetně logování min. 0,4 Gbps (měřeno na komunikaci typu mix aplikací)
* Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 0,2 Gbps
* Podpora SSL dekrypce/SSL inspekce s minimální propustností 0,1 Gbps (TLS 1.2AES 256-SHA, měřeno v kombinaci s IPS kontrolou)
* Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 200
* Propustnost IPSec VPN min. 2 Gbps (měřeno při AES 256)
* Minimální počet současně navázaných SSL VPN tunelů: 100
* Minimální propustnost SSL VPN: 0,1 Gbps

1. **Požadujeme pro stávající zařízení FG30E HW podporu na 5 let v režimu 7x24.**
2. **Součástí nabízeného řešení musí být Logovací a reportovací nástroj ve formě virtuální appliance pro platformu VMware s podporou výrobce na 5 let.**

**Základní technické požadavky**

* Logovací a reportovací nástroj
* Virtuální apliance pro platformu VMware vSphere (pro ver. 6 a vyšší)
* Podpora pro platformu Microsoft Hyper-V (ver. 2012 R2 a vyšší)
* Plná podpora pro nabízenou platformu NGFW
* Podpora pro Syslog kompatibilní zařízení
* Výkon logování min. 6 GB/den
* Kapacita storage (uložení historických dat) min. 3TB
* Real-time prohledávání logovaných dat
* Retrospektivní kontrola logů za využití aktuálních informací typu threat feeds, reputační databáze, apod.
* Vyhledávání historických dat podle typu události nebo typu provozu
* Vyhledávání podle zařízení
* Uživatelská definice reportů (vzhled, obsah apod.)
* Automatické generování reportů v daném čase a periodě
* Automatické odesílání reportů emailem