Příloha č. 3 Výzvy, č. 1 Smlouvy

**Technická specifikace vč. cenového souhrnu**

**Nákup bezpečnostních prvků Firewall pro Nemocnici Tábor, a.s.**

Zadavatelem stanovené minimální požadavky na předmět plnění jsou podmínkou zadavatele pro účast ve výběrovém řízení k zakázce 04/05/2025/OBCH „Nákup bezpečnostních prvků Firewall pro Nemocnici Tábor, a.s.“.

Účastník v technické specifikaci vyplní ve sloupci „**Požadovaná technická specifikace splněna ANO/ NE**“ ANO (splňuje) nebo NE (nesplňuje). Účastník do sloupce „**Nabízený produkt, funkce, parametr, poznámka**“ uvede nezaměnitelné označení konkrétního produktu (zejména označení názvu včetně typového označení, pokud ho zařízení má), dále účastník v tomto sloupci uvede konkrétní parametr/ hodnotu (velikost, kapacita, rychlost apod.) tak, aby bylo patrné, že nabízený produkt splňuje parametry požadované Zadavatelem a k nabídce přiloží detailní produktové listy nebo dokumentaci (např. „datasheet“ výrobce) v českém nebo anglickém jazyce ze kterých je možno uváděné vlastnosti/parametry ověřit. Zadavatel, níže v tabulce vymezuje buď konkrétní parametr, který musí být plněn s danou hodnotou nebo jinou charakteristikou, nebo vymezuje určitý parametr s minimální nebo maximální hodnotou, kterou nemůže účastník překročit/ podkročit, účastník musí uvést konkrétní hodnotu, kterou má nabízený produkt. V případě potřeby účastník do sloupce uvede také poznámku k technické specifikaci.

Účastník vyplní všechny požadované údaje v cenovém souhrnu.

# Cíl:

Cílem je obnova stávajících dosluhujících bezpečnostních prvků FIREWALL za nové. Dále pak udržení vysoké míry zabezpečení síťového provozu v souladu se Zákonem o kybernetické bezpečnosti.

# Stávající stav:

V současné době provozuje Nemocnice Tábor, a.s. dva hlavní identické Firewally z důvodu vysoké dostupnosti a dále dva menší Firewally pro VPN tunel do svých odloučených lokalit. Provozované modely byly výrobcem ukončeny v rámci jejich životního cyklu a již na ně nebudou vydávány bezpečnostní pravidla (UTM). Pořízení nových technologií je pro nemocnici kriticky nutné, vzhledem k ochraně dat a zabezpečení před kybernetickými hrozbami.

# Nevýhody stávajícího stavu:

Firewally jsou na konci svého životního cyklu. V nemocnici byly nepřetržitě provozovány od roku 2019. Již není možné zakoupit podporu výrobce na HW ani bezpečnostní pravidla (UTM).

# Obecné informace:

Poptávány jsou dva identické hlavní firewally v režimu Active-Active, pro zajištění komunikace LAN-LAN a LAN-WAN. A dva identické firewally kompatibilní s hlavními firewally v režimu VPN box pro odloučené lokality.

# **2x Firewall hlavní**

|  |  |  |
| --- | --- | --- |
| **Minimální technické požadavky na hardware a software, které zadavatel požaduje.** | **Požadovaná technická specifikace splněna ANO/ NE** | **Nabízený produkt, funkce, parametr, poznámka** |
| Základní technické požadavky: | * Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí min. firewall, SSL dekrypce, porovnávání se signaturovou databází)
* Celá dodávka musí obsahovat všechny HW 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.
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU
* Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu
* Možnost rozšíření platformy o další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem.
* Možnost rozšíření o platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.
 |  |  |
| HW parametry: | * Počet síťových rozhraní RJ45 10/100/1000 - min 8x
* Počet síťových rozhraní RJ45 2,5 GE – min 4x
* Počet síťových rozhraní RJ45 5 GE – min 4x
* Počet síťových rozhraní GE SFP – min 4x
* Počet síťových rozhraní 10 GE SFP+ - min 8x
* Konzolový port pro management
* Dedikovaný port RJ45 pro management
* Dedikovaný port RJ45 pro HA
* USB 3.0 port pro zálohu konfigurace
* Redundantní napájecí zdroj
 |  |  |
| Výkonnostní parametry: | * Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B – min 37 Gbps, 37 Gbps, 25 Gbps
* Výkon firewall – min. 38 000 000 paketů / s
* Počet současně otevřených spojení – min. 10 M
* Počet nových spojení za sekundu – min. 400 000
* Počet firewall pravidel až 10 000
* Latence firewallu (pro 64 B UDP paket) – max 4,5 mikrosekundy
 |  |  |
| *Networking a High Availibility:* | * Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru
* Režim fungování L2 – transparentní režim, L3 – NAT/Router
* Podpora VLAN
* Podopora multicast, vytváření politiky pro multicast routování
* Podpora 802.3ad link aggregation
* Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
* Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
* Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
* Policy-based routing
* Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky
 |  |  |
| *VPN:* | * **Funkce SSL VPN**
	+ Podpora klientského i bezklientského (portálového) režimu
	+ Minimální počet současně navázaných SSL VPN tunelů: 450
	+ Minimální propustnost SSL VPN: 3000 Mbps
* **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: 1900
	+ Minimální počet klientských IPSEC VPN tunelů: 15000
	+ propustnost IPSec VPN min. 35Gbps (měřeno při AES256-SHA256)
	+ podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
	+ podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
	+ podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
* Podpora VXLAN
* Podpora L2TP, PPTP, GRE
* podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec
 |  |  |
| *UTM:* | * **Funkce detekce aplikací na L7 (Application Control)**
	+ Detekce známých aplikací na základě signatur
	+ Signaturová databáze automaticky aktualizovaná výrobcem
	+ alespoň 4000 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
	+ funkce AppCtr se konfiguruje v rámci 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)**
	+ 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. 8.5 Gbps
* **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. 6 Gbps
	+ funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
	+ Podpora služby výrobce, která umožní́ detekovat malware, který byl objevený v době od poslední́ aktualizace AV signaturové databáze pomocí globální́ a rychle se aktualizující́ databáze hashů
	+ Funkce odstranění́ aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní́ emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
* **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 předchozího bodu)
	+ Možnost definovat vlastní tzv. blacklist domén
	+ Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
	+ Možnost importu seznamu blokovaných domén do DNS filtru
	+ Detekce a blokování komunikace do botnet sítí
* Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty
* Podpora SSL dekrypce/SSL inspekce s minimální propustností 6000 Mbps
* DoS Policy prevence proti základním útokům typu DoS
 |  |  |
| Funkce Firewall: | * Možnost nastavovat firewall politiku na základě geografických údajů
* Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
* Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
* Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
* Viditelnost do provozu na aplikační úrovni
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
* Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
* Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
* Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
* Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
* Podpora funkce reverzní proxy
* Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
* **Explicit proxy**
	+ podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl)
	+ podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
	+ funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
	+ Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru
 |  |  |
| Integrovaný kontroler bezdrátových sítí (Wi-Fi) | * Wifi kontroler integrovaný do NGFW platformy pro alespoň 120 AP (v tunelovém módu)
* Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroleru
* podpora bezpečnostních profilů (AV, AppControl, Webfilter) přímo na wifi kontroleru
* podpora SSL dekrypce uživatelského provozu přímo na wifi kontroleru
* Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení
* Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor, WiFi 6, WiFi 6e)
* Podpora BSS Coloring
* On-wire rogue AP detekce a mitigace
* Podpora fast-roamingu (802.11 k,v,r)
* podpora více PSK u jednoho SSID
* podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)
* Podpora WPA3 protokolu
 |  |  |
| Integrovaný switch Kontroler: | * Zařízení musí podporovat switch kontroler jenž umožní spravovat switche výrobce z jednoduchého GUI v počtu alespoň 60 přepínačů
* Možnost správy VLAN
* Spolu s NAC politikami musí nabídnout možnost automatické přiřazení VLAN pro konkrétní zařízení či skupinu zařízeních
* Z integrovaného switch kontroleru musí být obsluha schopna pomocí GUI jednoduše definovat VLAN na konkrétní port
* V případě správy switche s funkcí PoE musí být v GUI možnost resetování PoE pro vzdálený restart zařízení
 |  |  |
| Virtualiazce: | * Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
* Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
* Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)
 |  |  |
| Management: | * FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API
 |  |  |
| Požadované příslušenství: | * 2x 10Gbit/s Multimode (SR).
 |  |  |
| Licence: | * 5 let v rozsahu požadovaných funkcí.
 |  |  |
| Záruka a servisní pokrytí: | * 5 let s výměnou následující pracovní den, softwarová podpora včetně práva na nové verze (upgrade/update).
 |  |  |

# **2x Firewall VPN box:**

|  |  |  |
| --- | --- | --- |
| **Minimální technické požadavky na hardware a software, které zadavatel požaduje.** | **Požadovaná technická specifikace splněna ANO/ NE** | **Nabízený produkt, poznámka** |
| Základní technické požadavky: | * Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …)
* Celá dodávka musí obsahovat všechny HW 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.
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti desktop
* Možnost rozšíření platformy o další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem.
* Možnost rozšíření o platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.
 |  |  |
| HW parametry: | * Počet síťových rozhraní RJ45 10/100/1000 - min 5x
* Konzolový port pro management
* USB 3.0 port pro zálohu konfigurace
 |  |  |
| Výkonnostní parametry: | * Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 4500 Mbps, 4500 Mbps, 4500 Mbps
* Latence firewallu (64 B UDP paket) - max 3,5 mikro sec
* Výkon firewall – min. 7 000 000 paketů / s
* Počet naráz otevřených spojení – min 650 000
* Počet nových spojení za sekundu - min. 32 000
* Počet firewall pravidel až 2 000
* Podpora virtualizace (min 10 virtuálních kontextů)
* Podpora funkce bezdrátový kontrolér (tunelový mód) – min 8 AP
* Podpora funkce integrovaný switch controller – podpora 8 switchů
 |  |  |
| *Networking a High Availibility:* | * Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru
* Režim fungování L2 – transparentní režim, L3 – NAT/Router
* Podpora VLAN
* Podopora multicast, vytváření politiky pro multicast routování
* Podpora 802.3ad link aggregation
* Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
* Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
* Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
* Policy-based routing
* Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky
 |  |  |
| VPN: | * **Funkce SSL VPN**
	+ Podpora klientského i bezklientského (portálového) režimu
	+ Minimální počet současně navázaných SSL VPN tunelů: 180
	+ Minimální propustnost SSL VPN: 450Mbps
* **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: 180
	+ Minimální počet klientských IPSEC VPN tunelů: 220
	+ propustnost IPSec VPN min. 4 Gbps (měřeno při AES256-SHA256)
	+ podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
	+ podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
	+ podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
* Podpora VXLAN
* Podpora L2TP, PPTP, GRE
* podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec
 |  |  |
| UTM: | * **Podpora funkcí detekce aplikací na L7 (Application Control)**
	+ Detekce známých aplikací na základě signatur
	+ Signaturový database automaticky aktualizované výrobcem
	+ alespoň 4000 podporovaných aplikací
	+ pro populárná 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
	+ funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.
* **Podpora funkcí 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. 900Mbps (měřeno na komunikaci typu mix aplikací)
* **Podpora funkcí 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 lokálné HW appliance stejného výrobce
	+ deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 550 Mbps
	+ funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
	+ Podpora služby výrobce, která umožní detekovat malware, který byl objevený 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/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
* **Podpora funkcí 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
* **Podpora funkcí DNS filtru**
	+ Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)
	+ Možnost definovat vlastní tzv. blacklist domén
	+ Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
	+ Možnost importu seznamu blokovaných domén do DNS filtru
	+ Detekce a blokování komunikace do botnet sítí
* Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty
* Podpora SSL dekrypce/SSL inspekce s minimální propustností 300Mbps
* DoS Policy prevence proti základním útokům typu DoS
 |  |  |
| Firewall: | * Možnost nastavovat firewall politiku na základě geografických údajů
* Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
* Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
* Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
* Viditelnost do provozu na aplikační úrovni
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
* Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
* Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
* Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
* Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
* Podpora funkce reverzní proxy
* Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
* **Explicit proxy**
	+ podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
	+ podpora transparentního ověřování uživatelů proti MS AD protokolem Kerberos
	+ funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
	+ Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru
 |  |  |
| Integrovaný controller bezdrátových (Wifi) sítí: | * Wifi controller integrovaný do NGFW platformy
* Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním
* podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru
* podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru
* Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení
* Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor)
* On-wire rogue AP detekce a mitigace
* Podpora fast-roamingu (802.11 k,v,r)
* podpora více PSK u jednoho SSID
* podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)
* podpora WPA3 šifrování
 |  |  |
| *Virtualiazce:* | * Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
* Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
* Každý virtuální kontext je zároveň samostatným wifi controllerem
* Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)
 |  |  |
| Management: | * FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
* 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)
 |  |  |
| Licence: | * 5 let v rozsahu požadovaných funkcí.
 |  |  |
| Záruka a servisní pokrytí: | * 5 let s výměnou následující pracovní den, softwarová podpora včetně práva na nové verze (upgrade/update).
 |  |  |

# **Implementační služby:**

|  |  |  |
| --- | --- | --- |
| **Zadavatel požaduje níže uvedené instalační a implementační služby**  | **Požadovaná technická specifikace splněna ANO/ NE** | **Nabízený produkt, poznámka** |
| *Instalační práce:* | * Instalace do datových rozvaděčů a příprava kabeláže.
* Konfigurace obou zařízení do HA.
 |  |  |
| *Příprava implementace v rozsahu:* | * Konfigurace všech požadovaných rozhraní.
* Konfigurace objektů do pravidel.
* Konfigurace zón.
* Konfigurace požadovaných pravidel pro LAN.
* Nastavení překladů NAT z Internetu do LAN.
* Konfigurace VPN (SSL, IPSec) pro koncové uživatele.
* Příprava konfigurace pro připojení na AD.
* Konfigurace UTM profilů (antivir, antispam, URL filtr, rychlostní limity, aplikační filtry, IPS atd.).
* Generování certifikátů, import certifikátů z externích autorit.
* Konfigurace SSL inspekce.
* Nastavení Logování do Syslogu a napojení na LOGMANAGER
 |  |  |
| *Testovací fáze:* | * Test chování firewallu v LAN prostředí (funkčnost zón, pravidel) před ostrým nasazením (s využitím nepoužívaných VLAN a napojením na internet přes stávající řešení).
* Test chování firewallu vůči aplikacím při zapnutých UTM profilech.
* Test chování přístupu běžného uživatele a uživatele s otevřenějším profilem vůči internetu (ověření SSL inspekce a jejího chování).
* Test HA.
 |  |  |
| *Nasazení do ostrého provozu:* | * Přepojení na hranici LAN-WAN (odstavení stávajícího LAN-WAN firewallu).
* Postupné přidávání lokálních LAN segmentů do firewallu.
 |  |  |
| *Zaškolení:* | * Požadováno v rozsahu min. 3 dnů.
 |  |  |
| *Pomigrační podpora:* | * Rozšířená post-instalační podpora v rozsahu 5 MD\*\* po záruční dobu a za podmínek uvedených v příloze č. 3 Smlouvy
 |  |  |

# Cenový souhrn:

|  |
| --- |
| **Dodavatelem/Prodávajícím nabízená kupní cena (Dodavatel/Prodávající vyplní žlutě podbarvená pole)** |
| **Druh dodávky** | **Cena za 1 ks/ kpl/MD (Kč bez DPH)**  | **Počet ks/kpl/MD** | **sazba DPH** | **Cena celkem (Kč bez DPH)** | **Cena celkem (Kč vč. DPH)** |
| Hlavní Firewall\*  |  | **2**  |  |  |  |
| Firewall VPN\* box |  | **2**  |  |  |  |
| Implementační a konfigurační práce |  | **1 kpl** |  |  |  |
| Pomigrační podpora |  | **5 MD** |  |  |  |
| **CELKEM** |  |  |

\*Cena za tuto položku bude zahrnovat i servisní podporu.

\*\***1 MD odpovídá 8 hodinám práce jedné osoby**. Zadavatel si vyhrazuje právo využít této služby dle svých aktuálních potřeb v uvedeném časovém období. Podpora je již kalkulována v Ceně dle odst. 3.1. Smlouvy. Do čerpání služby pomigrační podpory se započítává výhradně skutečně odpracovaný čas (nikoli celý MD za jednotlivou dílčí konzultaci).