Příloha č. 1 - Specifikace předmětu plnění												
Kód	**Název položky**	**Minimální požadované specifikace**	**Počet ks**	**Výrobce a typ nabízeného zboží**	**Specifikace nabízeného zboží**	**Cena za 1 jednotku bez DPH**	**Celková nabídková cena za položku bez DPH**	**Maximální možná cena položky bez DPH**	**Žadatel o položku**	**Příkazce operace**	**Zakázka**	**Pracoviště**	**Místo doručení; kontakní osoba**
1	Firewall - Fyzický HW	požadavky dle Přílohy č. 1A - Technické specifikace předmětu plnění	1	Fortinet FortiGate 500E, FortiAnalyzer 200F, FortiSandbox 1000D	**2x FortiGate 500E** 2 x 10GE SFP+ slots, 10 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 8 x switch ports), 8 x GE SFP slots, SPU NP6 and CP9 hardware accelerated **FortiAnalyzer 200F** Centralized log & analysis appliance - 2 x GE RJ45, 4TB storage, up to 100GB/Day of logs. **FortiSandbox 1000D** Advanced Threat Protection System - 6 x GE RJ45, 2 x GE SFP slots, redundant PSU, 8 VMs with Win7 and (1) MS Office License included, Upgrade FSA-1000D to support Windows 8/10 - Win8 / Win10 license included	**1 082 720**	**1 082 720,00 Kč**	1 098 880,00 Kč					
2	Firewall - Podpora (UTM funkce)	požadavky dle Přílohy č. 1A - Technické specifikace předmětu plnění	1	Fortinet UTM funkcionality, podpora na požadované období	**FG500E** UTM Protection (8x5 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam Services) (2x) **FAZ200F** 24x7 FortiCare Contract **FSA1000D** 24x7 FortiCare plus FortiGuard Threat Intelligence (AV, IPS, Web Filtering, File Query and SandBox Engine Updates)	**1 968 180**	**1 968 180,00 Kč**	1 973 350,00 Kč					
						Předpokládaná hodnota veřejné zakázky bez DPH		3 072 230,00 Kč					
						Celková nabídková cena za veřejnou zakázku bez DPH		**3 050 900,00 Kč**					

Firewall

Poptáváme **komplexní řešení** Next Generation firewall kombinované s kolektorem logů, který bude zároveň umožňovat jejich analýzu a reporting. Jako součást řešení také poptáváme zařízení typu sandbox pro detekci a analýzu pokročilých hrozeb. Licence všech níže požadovaných funkcionalit a podpora celého řešení musí být platná do 31. 12. 2022. Součástí dodávky bude provedení instalace, konfigurace a zprovoznění nového řešení, včetně migrace stávající konfigurace a bezpečnostních pravidel. Požadujeme rovněž zaškolení obsluhy na celé poptávané řešení minimálně pro 3 osoby.

Next Generation Firewall

Poptáváme vysoce dostupné řešení (2x HW zařízení) typu Next Generation firewall, které bude s funkcí stavového paketového filtru kombinovat řadu dalších síťových a bezpečnostních funkcí.

HW parametry:

- NGFW firewall ve formě HW appliance.
  - Termínem HW appliance rozumíme operační systém i aplikaci vytvořenou pro specifický HW, určený přímo pro funkci NGFW. Tento celek bude krytý stejnou servisní smlouvou.
  - Řešení postavené na virtuální appliance nebo na software instalovaný na obecný server nebude akceptováno.
- Počet síťových rozhraní typu 10GbE SFP+: min. 2.
- Počet síťových rozhraní typu 1GE RJ-45: min. 8.
- Počet síťových rozhraní typu 1GE SFP: min. 8.
- Počet dedikovaných 1GE RJ-45 management portů: min. 1.

Výkonnostní parametry:

- Propustnost FW (stavové filtrování, UDP paket) – min. 30 Gbps.
- Latence firewallu (64 B UDP paket) – max. 3.5 µs.
- Počet současně otevřených spojení – min. 5 000 000.
- Počet nových spojení za sekundu - min. 200 000.
- Propustnost NGFW (při současně zapnutých ochranách typu FW, IPS a Application visibility & control, měřeno na datovém toku emulujícím reálný provoz v prostředí enterprise): min. 5 Gbps.
- Propustnost IPSEC VPN (512B paket, AES-256/SHA-256) - min. 20 Gbps.
- Propustnost SSL VPN – min. 4,5 Gbps.
- Propustnost SSL inspekce (TLS v1.2 + AES128-SHA256) - min. 6 Gbps.
- Minimální počet kategorií pro URL filtraci, udržovaných výrobcem: 80.

Požadavky na síťové a bezpečnostní funkce:

- Režim vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a SA mezi nody v clusteru.
- Podpora virtualizace. Možnost tvorby virtuálních instancí se samostatnou konfigurací a správou přímo na daném HW. V rámci dodávky musí být zajištěna podpora min. 10 virtuálních instancí, včetně kompletní podpory na úrovni aplikačních kontrol (AV, IPS, Application Control, URL filtrace).
- Režim fungování L2 – transparentní režim, L3 – NAT/Router. Toto je požadováno včetně kombinace s virtualizací, tedy každá virtuální instance může být nakonfigurována libovolně v L2 nebo L3 režimu.
- Podpora multicast, vytváření politiky pro multicast routování.
- Podpora 802.3ad link aggregation.
- Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet

browsing konfigurace), podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu, podpora IPv6.
- Firewall, podpora VXLAN, podpora dynamicky navazovaných tunelů dle potřeby komunikace.
- Možnost nastavovat firewall politiku na základě geografických údajů.
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru.
- Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálné servery, podpora health check funkcí, podpora SSL offload.
- Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace.
- Viditelnost do provozu na aplikační úrovni.
- UTM funkce – IPS, Application visibility & control, anti-malware, URL filtrace.
- Antivirus pro vybrané protokoly, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger). Signaturová databáze udržovaná výrobcem po dobu platné podpory.
- Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty.
- Intrusion Protection System – detekce útoků založena na signaturové části a na anomálním filtru (ochrana proti útokům typu DoS), možnost vytvářet vlastní signatury. Signaturová databáze udržovaná výrobcem po dobu platné podpory, minimální počet 10.000 signatur v aktuální verzi databáze.
- Funkcionalita Web Filtru – založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne. Databáze kategorizovaných URL udržovaná výrobcem.
- Data Leak Prevention s funkcí document fingerprinting.
- Reputační databáze obsahující známe IP adresy a domény C&C Botnet sítí.
- Application Control – detekce, monitoring, povolení či zakázání vice než 3000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu. Databáze signatur udržovaná výrobcem. Možnost tvorby vlastních signatur.
- Deep scanning – možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S).
- DoS Policy prevence proti základním útokům typu DoS, syn proxy.
- Ověřování uživatelů LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu.
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
- Podpora dynamických routovacích protokolů – min. RIP, BGP, OSPF, IS-IS.
- Policy routing.
- Traffic Shaping, QoS s podporou DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii.
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu.
- Explicitní Proxy, Reverzní proxy, WCCP.
- Podpora funkce explicit proxy, podpora autentizace protokolem Kerberos při využití funkce explicit proxy.
- Podpora silné autentizace uživatele (na bázi jednorázových hesel generovaných pomocí tokenů), zejména administrátorů a uživatelů připojujících se pomocí VPN. Součástí dodávky musí být kompletní řešení pro 2FA ověřování administrátorů pomocí generátoru jednorázových hesel instalovaných na mobilní telefony pro minimálně 2 administrátory. Po další fázi pak požadujeme možnost jednoduchého licenčního rozšíření na vyšší počet uživatelů.

Podpora:

- Požadujeme podporu v režimu 8x5 na obě zařízení se zahrnutím podpory také na aplikační a antispamovou kontrolu, IPS, AV, Web Filtering.

Systém pro ukládání, analýzu a korelaci logů

Je poptáván systém pro ukládání a korelaci logů v síti zadavatele. Systém musí být plně kompatibilní s dodávaným firewallem a platformou sandbox a musí plně podporovat analýzu logů z daného prostředí. Dále musí být schopný poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.
Plná funkční kompatibilita s firewallem a sandbox platformou musí být oficiálně doložena výrobcem těchto platforem.

- Požadujeme HW appliance o velikosti 1RU.
  - Termínem HW appliance rozumíme operační systém i aplikaci vytvořenou pro specifický HW určený přímo pro funkci ukládání a korelaci logů. Tento celek bude krytý stejnou servisní smlouvou.
  - Řešení postavené na virtuální appliance nebude akceptováno.
- Plná podpora NGFW i sandbox platformy, dodávané v rámci tohoto tendru.
- Požadujeme obousměrnou komunikaci mezi FW a logovací platformou. Obousměrnou komunikací rozumíme možnost prohledávat logy, uložené na logovací platformě přímo z GUI prostředí firewallu.
- Kapacita úložiště min. 4TB.
- Řešení musí být schopno přijímat minimálně 80 GB logů za den. Pokud je pro dosažení této hodnoty vyžadována licence, tak tato musí být součástí dodávky.
- Výkonnost řešení musí zaručit příjem min. 2 800 událostí/sec. Pokud je pro dosažení této hodnoty vyžadována licence, tak tato musí být součástí dodávky.
- Možnost rozdělení zařízení na oddělené administrativní sekce (každá virtuální instance firewallu může být v jiné administrativní sekci centrálního logovacího zařízení).
- Možnost dostat se z vizuálního zobrazení ke konkrétním logům jednoduchým proklikem.
- Možnost prohlížení a prohledávání historických logů stejně jako logů v reálném čase.
- Korelace logů.
- Samostatná sekce informující o hrozbách v síti.
- Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF.
- Generování reportů v pravidelných intervalech.
- Předdefinované vzory pro reporty na nejčastější použití.
- Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze.
- Podpora prohlížení statistických údajů nad logy.
- Upozorňování na důležité informace z logů – emailem a SNMP trapy.
- Event Management.
- Předpřipravený dashboard pro využití dohledovým centrem.
- Možnost rozšíření o funkci retrospektivní kontroly logů za využití aktuálních informací typu threat feeds, reputační databáze, atd.

Podpora:

- Požadujeme podporu v režimu 24x7

Sandbox

Je poptáván systém typu sandbox, pro detekci a analýzu pokročilých hrozeb plně kompatibilní s nabízenou platformou NGFW.

HW parametry:

- Forma HW appliance
  - Termínem HW appliance rozumíme operační systém i aplikaci vytvořenou pro specifický HW, určený přímo pro funkci sanboxingu. Tento celek bude krytý stejnou servisní smlouvou.
  - Řešení postavené na virtuální appliance nebo na software instalovaným na obecný server nebude akceptováno.
- Max. velikost 2RU.
- Síťová rozhraní
  - 6x 1GE RJ45,
  - 2x 1GE SFP.
- Lokální disková kapacita min. 2 TB.

Požadavky na funkce:

- Součástí dodávky musí být min. 8 paralelně běžících virtuálních operačních systémů běžně provozovaných v síti zadavatele (uvedeno níže), plně pokrytých licencemi.
- Součástí dodávky musí být licence na min. 1 ks MS Office.
- podpora HA režimu:
  - cílem je zvýšení dostupnosti i rozkládání zátěže mezi více prvků,
  - požadujeme možnost povýšit celé řešení do režimu HA dodáním druhého modelu stejného typu.
- Podporované operační systémy minimálně:
  - MS Windows 7,
  - MS Windows 8/8.1,
  - MS Windows 10,
  - Android.
  - Možnost importu připravené verze OS, emulující standardní instalaci v prostředí zadavatele.
- Vícevrstvá ochrana/detekce škodlivého kódu minimálně za pomoci signaturové AV kontroly, plnohodnotného sandboxingu a detekce komunikace s C&C servery.
- Pokročilé techniky typu anti-evasion.
- Podpora kontroly minimálně následujících typů souborů:
  - spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např. JPEG, QuickTime, MP3; archívy (ZIP/RAR/7ZIP/TNEF), asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv.
- Požadované možnosti integrace do síťové infrastruktury:
  - Integrace na SPAN switche / zařízení typu TAP.
  - Podpora protokolu ICAP.
  - Integrace přes sdílené disky (CIFS, NFS).
  - Otevřené API (plná možnost integrace do stávajících web aplikací pomocí API).
  - Nativní integrace s bezpečnostními prvky dodávanými v rámci této zakázky.
  - Všechny výše uvedené metody musí být využitelné naráz a na jedné appliance. Pokud je pro jakékoliv z těchto metod nutná dodatečná licence, tak tato musí být součástí dodávky.
- Síťové rozhraní vyhrazené pro management (1GE, RJ-45).
- Plnohodnotný lokální management (GUI & CLI) dostupný přes protokoly HTTPS a SSH, bez nutnosti instalovat management aplikaci nebo management server.
- Automatická aktualizace signaturových databází.
- Aktualizace virtuálních operačních systémů plně udržované výrobcem.

- Dedikované síťové rozhraní pro přístup VM do Internetu (1GE).
- Funkce logování a reporting přímo na sandbox appliance.
- Podpora reportování ve standardních formátech (HTML, CSV, PDF, XML).

Výkonnostní parametry:

Požadujeme výrobcem definovanou výkonnost zvlášť pro klasickou AV ochranu, zvlášť pro plnohodnotný sandboxing a zvlášť pro provoz v reálném prostředí. Tyto minimální hodnoty musí být doložené oficiálním produktovým listem výrobce.

- 8 paralelně běžících operačních systémů,
- 5.000 souborů/hod při klasické AV kontrole (kontrola proti signaturové DB),
- 150 souborů/hod při plné sandbox kontrole,
- 450 souborů/hod pro reálný provoz.

Podpora:

Požadujeme podporu v režimu 24x7 se zahrnutím podpory také na AV, IPS, Web Filtering, reputačních databází pro kontrolu souborů a SW aktualizace sandboxu.