Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

Tabuľka č. 1

Podrobná špecifikácia požadovaných firewallov

Minimálne požiadavky verejného obstarávateľa	Ponuka uchádzača
Firewall typ A	
Výrobca a ponúkaný model firewallu	***PaloAltoNetworks PA-3220***
Priepustnosť firewallu minimálne 4 Gbps*	**4,8Gbps (appmix)**
Priepustnosť Threat prevention minimálne 2 Gbps*	**2,6Gbps (appmic)**
Priepustnosť IPsec VPN minimálne 2 Gbps*	**2,6 Gbps**
Maximálny počet súbežných spojení minimálne 800 000	**1000000**
Počet nových spojení za sekundu minimálne 50 000	**52800**
Rozmery maximálne 2U	**2U**
Porty pre správu firewallu minimálne 1 x 10/100/1000 out-of-band management port, minimálne 2 x 10/100/1000 high availability, minimálne 1 x 10G SFP+ high availability, minimálne 1 x RJ-45 console port, minimálne 1 x Micro USB	**1x management 10/100/1000 2xHA 10/100/1000 1x HA SFP+ 1x serial console RJ-45 1x microUSB**
Prevádzkové porty minimálne 12 x 10/100/1000 ethernet, minimálne 4 x 1G SFP, minimálne 4 x 1G/10G SFP/SFP+	**12x 10/100/1000 GE RJ-45 4x 1G SFP 4x10G SFP+**
Interné úložisko minimálne 200 GB SSD	**240GB SSD**
Firewall musí byť plnohodnotne integrovateľný do existujúceho systému centrálnej správy Palo Alto Networks Panorama u verejného obstarávateľa, t.j. musí zabezpečiť akceptáciu všetkých systémových nastavení, aktualizácií, politík, bezpečnostných profilov a konfigurácií NAT prostredníctvom existujúceho systému **	**Áno**
Firewall musí byť ako celok zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu a sandbox definícií	**Áno**
Podpora firewallu musí byť zaistená minimálne po dobu plánovanej životnosti firewallu určenú výrobcom	**Áno min 5 rokov po ukončení predaja**
Firewall musí byť typu HW zariadenie	**Áno**
Modul pre spracovanie dát musí byť v architektúre firewallu hardvérovo oddelený od ďalších podporných modulov (správa zariadenia a riadiaci modul pre podporné sieťové činnosti), aby nemohlo dôjsť k ich vzájomnému ovplyvneniu	**Áno obsahuje samostatný management plane a datatplane**
Firewall musí podporovať agregáciu portov pomocou protokolu 802.3ad (Link Aggregation Control Protocol)	**Áno**
Firewall musí byť rozmerovo kompatibilný s 19" rozvádzačom	**Áno, obsahuje kin na inštaláciu do racku 19“**
Firewall musí podporovať minimálne dva nezávislé redundantné zdroje napájania AC 230V	**Áno obsahuje 2 zdroje**
Firewall musí plne podporovať IPv4 a IPv6	**Áno podporuje**
Firewall musí podporovať zapojenie v režimoch linkovej vrstvy (s virtuálnym sieťovým rozhraním), sieťovej vrstvy, transparentný a TAP	**Áno podporuje L3, L2, TAP a virtual wire módy**

Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

Firewall musí podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64	**Áno** **(IPv4): static IP, dynamic IP, dynamic IP and port (port address translation-PAT) NAT64, NPTv6** **Ďalšie vlastnosti:** **dynamic IP reservation, tunable dynamic IP and port oversubscription**
Firewall musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding)	**Áno** **OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing** **Policy-based forwarding** **Point-to-Point Protocol over Ethernet (PPPoE)** **Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3**
PBF musí byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, používateľ	**Áno**
Firewall musí podporovať site-to-site VPN pomocou protokolu IPSec	**Áno** **Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)** **Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)** **Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512**
Firewall musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS)	**Áno**
Počet súčasne pripojených užívateľov prostredníctvom VPN nesmie byť licenčne obmedzený	**Počet (ani celkový ani súčasný) nie je licenčne obmedzený**
Firewall musí podporovať identifikáciu aplikácií naprieč všetkými portami/protokolmi	**Áno je to štandarná funkcionalita PANOS**
Identifikácia aplikácie musí prebiehať priamo vo Firewalle	**Áno je to štandarná funkcionalita PANOS**
Firewall musí detegovať a zabrániť aplikácii meniť porty, tzv. Port-hopping	**je to štandarná funkcionalita PANOS**
Firewall musí podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít	**Áno** **UserID je súčasťou PANOS**
Firewall musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotného HW zariadenia	**Áno** **Pre MS active directore a novel edirectory je podporovaný agentless mód, extrakcia identity zo syslogu prípadne XML API**
Firewall musí podporovať dešifrovanie odchádzajúcej SSL/TLS prevádzky	

Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

	Áno, dešifrovanie je podporované
Firewall musí podporovať dešifrovanie prichádzajúcej SSL/TLS prevádzky	**Áno, podporuje**
Firewall musí podporovať funkciu SSH proxy a kontrolovať tunelované aplikácie	**Áno, podporuje**
Firewall musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky	**Áno, podporuje**
Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom SMTP, HTTP, FTP, IMAP, POP3 a SMB	**Áno, podporuje**
Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania Firewallu	**Áno, s wildfire subskripciou je report prístupný priamo z logu**
Aktualizácia zero-day signatúr musí byť každých minimálne 5 minút inštalovaná do firewallu	**Áno, Podporované sú real-time aj každú minútu**
Firewall musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - whitelisting iba povolených aplikácií a zákaz všetkého ostatného, vrátane neznámej prevádzky	**Áno, Firewall povoľuje iba explicitne vydefinovanú komunikáciu**
Firewall musí obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (intrusion prevention system - IPS). Databáza IPS signatúr musí byť uložená priamo vo Firewalle. Aplikácia IPS profilu musí byť granulárna, na úrovni bezpečnostného pravidla	**Áno, je súčasťou Threat prevention subskripcie**
Firewall musí obsahovať integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr musí byť uložená priamo vo Firewalle. Aplikácia AV profilu musí byť granulárna, na úrovni bezpečnostného pravidla	**Áno, je súčasťou Threat prevention subskripcie**
Firewall musí byť schopný zisťovať prítomnosť vírusov a škodlivého kódu v dátovom toku minimálne v týchto aplikáciách: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB	**Áno**
Firewall musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu/uchádzača	**Áno**
Firewall musí podporovať možnosť zablokovania útoku využívajúceho známe Command and Control centrá aj v prípade, že je prevádzka šifrovaná a nie je možné vykonávať SSL dešifrovanie	**Áno Prostredníctvon DNS alebo URL subskripcie**
Firewall musí poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu	**Áno, podporuje**
Firewall musí obsahovať natívnu službu pre ochranu proti útoku typu DoS pomocou limitácie počtu spojení na úrovni zdrojová a cieľová IP adresa, užívateľská identita a aplikácia	**Áno, podporuje**
Firewall musí poskytovať možnosť obmedzenia využívanej šírky pásma na základe zdrojovej a cieľovej IP adresy, portu, užívateľskej identity, aplikácie a času (od - do, deň v týždni + čas)	**Áno, podporuje**

Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

Firewall musí obsahovať natívnu podporu pre využívanie databázy URL	**Áno URL kategória môže byť súčasťou porovnávacích kritérií v pravidle**
Firewall musí obsahovať lokálne úložisko záznamov	**Áno lokálny SSD disk**
Firewall musí obsahovať nástroj na analýzu záznamov bez nutnosti využitia ďalšieho systému mimo vlastného grafického používateľského prostredia	**Áno prehliadač záznamov je súčasťou rozhrania**
Firewall musí podporovať preposielanie záznamov na zariadenia tretích strán	**Áno, konfigurovateľný formát syslog**
Firewall musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov	**Áno, licenčný model závisí na výkonnosti HW, nie je zvislý na počte chránených IP alebo používateľov**
Firewall typ B	
Výrobca a ponúkaný model firewallu	***PaloAltoNetworks PA-220***
Priepustnosť firewallu minimálne 500 Mbps*	**540Mbps (appmix)**
Priepustnosť Threat prevention minimálne 300 Mbps *	**320 Mbps (appmix)**
Priepustnosť IPsec VPN minimálne 500 Mbps *	**540Mbps**
Maximálny počet súbežných spojení minimálne 60 000	**64000**
Počet nových spojení za sekundu minimálne 4 000	**4300**
Rozmery maximálne 1U	**1U / polovičná šírka**
Porty pre správu firewallu minimálne 1 x 10/100/1000 out-of-band management port, minimálne 1 x RJ-45 console port, minimálne 1 x Micro USB	**1x management 10/100/1000** **1x serial console RJ-45** **1x microUSB**
Prevádzkové porty minimálne 8 x 10/100/1000 ethernet	**8x 10/100/1000 GE RJ-45**
Interné úložisko minimálne 32 GB	**32GB eMMC**
Firewall musí byť plnohodnotne integrovateľný do existujúceho systému centrálnej správy Palo Alto Networks Panorama u verejného obstarávateľa, t.j. musí zabezpečiť akceptáciu všetkých systémových nastavení, aktualizácií, politík, bezpečnostných profilov a konfigurácií NAT prostredníctvom existujúceho systému **	**Áno**
Firewall musí byť ako celok zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu a sandbox definícií	**Áno**
Podpora firewallu musí byť zaistená minimálne po dobu plánovanej životnosti firewallu určenú výrobcom	**Áno**
Firewall musí byť typu HW zariadenie	**Áno**
Modul pre spracovanie dát musí byť v architektúre firewallu hardvérovo oddelený od ďalších podporných modulov (správa zariadenia a riadiaci modul pre podporné sieťové činnosti), aby nemohlo dôjsť k ich vzájomnému ovplyvneniu	**Áno**
Firewall musí podporovať agregáciu portov pomocou protokolu 802.3ad (Link Aggregation Control Protocol)	**Áno, podporuje**
Firewall musí byť rozmerovo kompatibilný s 19" rozvádzačom	**Áno**
Firewall musí podporovať minimálne dva nezávislé redundantné zdroje napájania AC 230V	**Áno, druhý zdroj je voliteľný**
Firewall musí plne podporovať IPv4 a IPv6	**Áno**

Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

Firewall musí podporovať zapojenie v režimoch linkovej vrstvy (s virtuálnym sieťovým rozhraním), sieťovej vrstvy, transparentný a TAP	**Áno podporuje L3, L2, TAP a virtual wire módy**
Firewall musí podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64	**Áno** **(IPv4): static IP, dynamic IP, dynamic IP and port (port address translation-PAT) NAT64, NPTv6** **Ďalšie vlastnosti: dynamic IP reservation, tunable dynamic IP and port oversubscription**
Firewall musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding)	**Áno** **OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing** **Policy-based forwarding** **Point-to-Point Protocol over Ethernet (PPPoE)** **Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3**
PBF musí byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, používateľ	**Áno**
Firewall musí podporovať site-to-site VPN pomocou protokolu IPSec	**Áno podporuje**
Firewall musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS)	**Áno podporuje**
Počet súčasne pripojených užívateľov prostredníctvom VPN nesmie byť licenčne obmedzený	**Počet (ani celkový ani súčasný) nie je licenčne obmedzený**
Firewall musí podporovať identifikáciu aplikácií naprieč všetkými portami/protokolmi	**Áno je to štandarná funkcionalita PANOS**
Identifikácia aplikácie musí prebiehať priamo vo Firewalle	**Áno je to štandarná funkcionalita PANOS**
Firewall musí detegovať a zabrániť aplikácii meniť porty, tzv. Port-hopping	**je to štandarná funkcionalita PANOS**
Firewall musí podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít	**Áno** **UserID je súčasťou PANOS**
Firewall musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotného HW zariadenia	**Áno** **Pre MS active directore a novel edirectory je podporovaný agentless mód, extrakcia identity zo syslogu prípadne XML API**
Firewall musí podporovať dešifrovanie odchádzajúcej SSL/TLS prevádzky	**Áno dešifrovanie je podporované**
Firewall musí podporovať dešifrovanie prichádzajúcej SSL/TLS prevádzky	**Áno podporuje**
Firewall musí podporovať funkciu SSH proxy a kontrolovať tunelované aplikácie	**Áno podporuje**

Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

Firewall musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky	**Áno podporuje**
Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom SMTP, HTTP, FTP, IMAP, POP3 a SMB	**Áno podporuje**
Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania Firewallu	**Áno, s wildfire subskripciou je report prístupný priamo z logu**
Aktualizácia zero-day signatúr musí byť každých minimálne 5 minút inštalovaná do firewallu	**Áno, Podporované sú real-time aj každú minútu**
Firewall musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - whitelisting iba povolených aplikácií a zákaz všetkého ostatného, vrátane neznámej prevádzky	**Áno, Firewall povoľuje iba explicitne vydefinovanú komunikáciu**
Firewall musí obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (intrusion prevention system - IPS). Databáza IPS signatúr musí byť uložená priamo vo Firewalle. Aplikácia IPS profilu musí byť granulárna, na úrovni bezpečnostného pravidla	**Áno, je súčasťou Threat prevention subskripcie**
Firewall musí obsahovať integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr musí byť uložená priamo vo Firewalle. Aplikácia AV profilu musí byť granulárna, na úrovni bezpečnostného pravidla	**Áno, je súčasťou Threat prevention subskripcie**
Firewall musí byť schopný zisťovať prítomnosť vírusov a škodlivého kódu v dátovom toku minimálne v týchto aplikáciách: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB	**Áno uvedené protokoly sú podporované**
Firewall musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu/uchádzača	**Áno umožňuje**
Firewall musí podporovať možnosť zablokovania útoku využívajúceho známe Command and Control centrá aj v prípade, že je prevádzka šifrovaná a nie je možné vykonávať SSL dešifrovanie	**Áno podporuje**
Firewall musí poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu	**Áno podporuje**
Firewall musí obsahovať natívnu službu pre ochranu proti útoku typu DoS pomocou limitácie počtu spojení na úrovni zdrojová a cieľová IP adresa, užívateľská identita a aplikácia	**Áno podporuje**
Firewall musí poskytovať možnosť obmedzenia využívanej šírky pásma na základe zdrojovej a cieľovej IP adresy, portu, užívateľskej identity, aplikácie a času (od - do, deň v týždni + čas)	**Áno podporuje**
Firewall musí obsahovať natívnu podporu pre využívanie databázy URL	**Áno URL kategória môže byť súčasťou porpovnývacích kritérií v pravidle**
Firewall musí obsahovať lokálne úložisko záznamov	**Áno lokálny SSD disk**

Príloha k časti B.1 „Opis predmetu zákazky“ – „Podrobný opis predmetu zákazky“

Firewall musí obsahovať nástroj na analýzu záznamov bez nutnosti využitia ďalšieho systému mimo vlastného grafického používateľského prostredia	**Áno prehliadač záznamov je súčasťou rozhrania**
Firewall musí podporovať preposielanie záznamov na zariadenia tretích strán	**Áno, konfigurovateľný formát syslog**
Firewall musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov	**Áno, licenčný model závisí na výkonnosti HW, ie je zývislý na počte chránených IP alebo používateľov**

* Všetky parametre priepustnosti musí uchádzač uvádzať v podmienkach reálnej prevádzky, tzv. "application mix"
** podrobné informácie o systéme centrálnej správy Palo Alto Networks Panorama sú uvedené na nasledovných odkazoch https://www.paloaltonetworks.com/resources/datasheets/panorama-centralized-management-datasheet a https://www.paloaltonetworks.com/resources/techbriefs/panorama-at-a-glance.html

Tabuľka č. 2

Podrobná špecifikácia požadovaných licencii a podpory k firewallom dodaným podľa tabuľky 1

Minimálne požiadavky verejného obstarávateľa	Ponuka uchádzača
Licencie a podpora pre firewally typ A na obdobie od 26.11.2021 do 19.3.2024	
Licencie pre službu ochrany pred hrozbami - pravidelné automatické aktualizácie signatúr známych hrozieb	**Áno**
Licencie sandbox riešenia so simuláciou a analýzou správania kódu v izolovanom prostredí	**Áno**
Hardvérová a softvérová podpora výrobcu, v rámci ktorej sa požaduje výmena zariadenia v prípade hardvérovej chyby, dodávka opravných balíkov, nových verzií operačného systému a riešenie technických problémov	**Áno**
Licencie pre bránu vzdialeného prístupu pre zabezpečenie virtuálnej privátnej siete	**Áno**
Licencie pre službu zabezpečenia DNS (domain name system)	**Áno**
Licencie a podpora pre firewally typ B na obdobie od 26.11.2021 do 19.3.2024	
Hardvérová a softvérová podpora výrobcu, v rámci ktorej sa požaduje výmena zariadenia v prípade hardvérovej chyby, dodávka opravných balíkov, nových verzií operačného systému a riešenie technických problémov	**Áno**
Licencie pre službu ochrany pred hrozbami - pravidelné automatické aktualizácie signatúr známych hrozieb	**Áno**
Licencie pre službu filtrovania škodlivých URL	**Áno**