Tabuľka č. 1

**Podrobná špecifikácia požadovaných firewallov**

|  |  |
| --- | --- |
| **Minimálne požiadavky verejného obstarávateľa** | **Ponuka uchádzača** |
| **Firewall typ A** |  |
| **Výrobca a ponúkaný model firewallu** |  |
| Priepustnosť firewallu minimálne 4 Gbps\* |  |
| Priepustnosť Threat prevention minimálne 2 Gbps\* |  |
| Priepustnosť IPsec VPN minimálne 2 Gbps\* |  |
| Maximálny počet súbežných spojení minimálne 800 000 |  |
| Počet nových spojení za sekundu minimálne 50 000 |  |
| Rozmery maximálne 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 |  |
| Prevádzkové porty minimálne 12 x 10/100/1000 ethernet, minimálne 4 x 1G SFP, minimálne 4 x 1G/10G SFP/SFP+ |  |
| Interné úložisko minimálne 200 GB 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 \*\* |  |
| 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 |  |
| Podpora firewallu musí byť zaistená minimálne po dobu plánovanej životnosti firewallu určenú výrobcom |  |
| Firewall musí byť typu HW zariadenie |  |
| 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 |  |
| Firewall musí podporovať agregáciu portov pomocou protokolu 802.3ad (Link Aggregation Control Protocol) |  |
| Firewall musí byť rozmerovo kompatibilný s 19" rozvádzačom |  |
| Firewall musí podporovať minimálne dva nezávislé redundantné zdroje napájania AC 230V |
| Firewall musí plne podporovať IPv4 a IPv6 |  |
| Firewall musí podporovať zapojenie v režimoch linkovej vrstvy (s virtuálnym sieťovým rozhraním), sieťovej vrstvy, transparentný a TAP |  |
| Firewall musí podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64 |  |
| Firewall musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding) |  |
| PBF musí byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, používateľ |  |
| Firewall musí podporovať site-to-site VPN pomocou protokolu IPSec |  |
| Firewall musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS) |  |
| Počet súčasne pripojených užívateľov prostredníctvom VPN nesmie byť licenčne obmedzený |  |
| Firewall musí podporovať identifikáciu aplikácií naprieč všetkými portami/protokolmi |  |
| Identifikácia aplikácie musí prebiehať priamo vo Firewalle |  |
| Firewall musí detegovať a zabrániť aplikácii meniť porty, tzv. Port-hopping |  |
| Firewall musí podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít |  |
| Firewall musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotného HW zariadenia |  |
| Firewall musí podporovať dešifrovanie odchádzajúcej SSL/TLS prevádzky |
| Firewall musí podporovať dešifrovanie prichádzajúcej SSL/TLS prevádzky |  |
| Firewall musí podporovať funkciu SSH proxy a kontrolovať tunelované aplikácie |  |
| Firewall musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky |  |
| Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom SMTP, HTTP, FTP, IMAP, POP3 a SMB |  |
| Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania Firewallu |  |
| Aktualizácia zero-day signatúr musí byť každých minimálne 5 minút inštalovaná do firewallu |  |
| Firewall musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - whitelisting iba povolených aplikácií a zákaz všetkého ostatného, ​​vrátane neznámej prevádzky |  |
| 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 |  |
| 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 |  |
| 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 |  |
| Firewall musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu/uchádzača |  |
| 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 |  |
| Firewall musí poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu |  |
| 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 |  |
| 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) |  |
| Firewall musí obsahovať natívnu podporu pre využívanie databázy URL |  |
| Firewall musí obsahovať lokálne úložisko záznamov |  |
| Firewall musí obsahovať nástroj na analýzu záznamov bez nutnosti využitia ďalšieho systému mimo vlastného grafického používateľského prostredia |  |
| Firewall musí podporovať preposielanie záznamov na zariadenia tretích strán |  |
| Firewall musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov |  |
| **Firewall typ B** |  |
| **Výrobca a ponúkaný model firewallu** |  |
| Priepustnosť firewallu minimálne 500 Mbps\* |  |
| Priepustnosť Threat prevention minimálne 300 Mbps \* |  |
| Priepustnosť IPsec VPN minimálne 500 Mbps \* |  |
| Maximálny počet súbežných spojení minimálne 60 000 |  |
| Počet nových spojení za sekundu minimálne 4 000 |  |

|  |  |
| --- | --- |
| Rozmery maximálne 1U |  |
| 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 |  |
| Prevádzkové porty minimálne 8 x 10/100/1000 ethernet |  |
| Interné úložisko minimálne 32 GB |  |
| 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 \*\* |  |
| 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 |  |
| Podpora firewallu musí byť zaistená minimálne po dobu plánovanej životnosti firewallu určenú výrobcom |  |
| Firewall musí byť typu HW zariadenie |  |
| 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 |
| Firewall musí podporovať agregáciu portov pomocou protokolu 802.3ad (Link Aggregation Control Protocol) |  |
| Firewall musí byť rozmerovo kompatibilný s 19" rozvádzačom |  |
| Firewall musí podporovať minimálne dva nezávislé redundantné zdroje napájania AC 230V |  |
| Firewall musí plne podporovať IPv4 a IPv6 |  |
| Firewall musí podporovať zapojenie v režimoch linkovej vrstvy (s virtuálnym sieťovým rozhraním), sieťovej vrstvy, transparentný a TAP |  |
| Firewall musí podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64 |  |
| Firewall musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding) |  |
| PBF musí byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, používateľ |  |
| Firewall musí podporovať site-to-site VPN pomocou protokolu IPSec |  |
| Firewall musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS) |  |
| Počet súčasne pripojených užívateľov prostredníctvom VPN nesmie byť licenčne obmedzený |  |
| Firewall musí podporovať identifikáciu aplikácií naprieč všetkými portami/protokolmi |  |
| Identifikácia aplikácie musí prebiehať priamo vo Firewalle |  |
| Firewall musí detegovať a zabrániť aplikácii meniť porty, tzv. Port-hopping |  |
| Firewall musí podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít |  |
| Firewall musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotného HW zariadenia |  |
| Firewall musí podporovať dešifrovanie odchádzajúcej SSL/TLS prevádzky |  |
| Firewall musí podporovať dešifrovanie prichádzajúcej SSL/TLS prevádzky |  |
| Firewall musí podporovať funkciu SSH proxy a kontrolovať tunelované aplikácie |  |
| Firewall musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky |  |
| Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom SMTP, HTTP, FTP, IMAP, POP3 a SMB |  |
| Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania Firewallu |  |
| Aktualizácia zero-day signatúr musí byť každých minimálne 5 minút inštalovaná do firewallu |  |
| Firewall musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - whitelisting iba povolených aplikácií a zákaz všetkého ostatného, ​​vrátane neznámej prevádzky |  |
| 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 |  |
| 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 |  |
| 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 |  |
| Firewall musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu/uchádzača |  |
| 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 |  |
| Firewall musí poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu |  |
| 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 |  |
| 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) |  |
| Firewall musí obsahovať natívnu podporu pre využívanie databázy URL |  |
| Firewall musí obsahovať lokálne úložisko záznamov |  |
| Firewall musí obsahovať nástroj na analýzu záznamov bez nutnosti využitia ďalšieho systému mimo vlastného grafického používateľského prostredia |  |
| Firewall musí podporovať preposielanie záznamov na zariadenia tretích strán |  |
| Firewall musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov |  |

\* 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 |  |

|  |  |
| --- | --- |
| Licencie sandbox riešenia so simuláciou a analýzou správania kódu v izolovanom prostredí |  |
| 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 |  |
| Licencie pre bránu vzdialeného prístupu pre zabezpečenie virtuálnej privátnej siete |  |
| Licencie pre službu zabezpečenia DNS (domain name system) |  |

|  |  |
| --- | --- |
| **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 |  |
| Licencie pre službu ochrany pred hrozbami - pravidelné automatické aktualizácie signatúr známych hrozieb |  |
| Licencie pre službu filtrovania škodlivých URL |  |