**Špecifikácia požiadavky na obstarávanie – položky č. 13 až 16 uvedené v kategórií č. 6**

Požadujú sa dva typy firewallov podľa nižšie uvedenej špecifikácie, spĺňajúce podmienku plnohodnotnej integrácie do existujúceho systému centrálnej správy Palo Alto Networks Panorama (<https://www.paloaltonetworks.com/resources/datasheets/panorama-centralized-management-datasheet>, https://www.paloaltonetworks.com/resources/techbriefs/panorama-at-a-glance.html), t.j. akceptáciu všetkých systémových nastavení, aktualizácií, politík, bezpečnostných profilov a konfigurácií NAT prostredníctvom existujúceho systému. Súčasťou predmetu zákazky pre firewall typu A budú licencie pre službu ochrany pred hrozbami - pravidelné automatické aktualizácie signatúr známych hrozieb, licencie sandbox riešenia so simuláciou a analýzou správania kódu v izolovanom prostredí, HW a SW podpora výrobcu pre firewall typ A (v rámci ktorej sa požaduje výmena zariadenia v prípade HW chyby, dodávka opravných balíkov, nových verzii OS a riešenie technických problémov), licencie vzdialených prístupov prostredníctvom firewallu typ A pre zabezpečenie virtuálnej privátnej siete a licencie pre službu zabezpečenia DNS. Pre firewall typu B budú predmetom zákazky licencie pre služby podpory výrobcu vrátane poskytovania aktualizácií, bezplatnej výmeny zariadenia pri poruche a dostupnosti technickej podpory v režime 24/7, licencie pre službu ochrany pred hrozbami a licencie pre filtrovanie URL adries.Bezpečnostné zariadenie typu firewall (ďalej tiež ako „FW“) musí byť z dôvodu efektívnosti jeho správy ako celok zložené z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií a pod. Zariadenia od viacerých výrobcov by spôsobili zvýšenie nárokov na správu systému ochrany siete MZVEZ. Zároveň musí byť týmto jedným výrobcom zaistená podpora minimálne po dobu plánovanej životnosti firewallu určenú výrobcom tohto firewallu.

Parametre, požiadavky na HW architektúru a funkcionalita:

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Firewall typ A** | **Firewall typ B** |
| Priepustnosť FW | minimálne 4 Gbps | minimálne 500 Mbps |
| Priepustnosť Threat prevention | minimálne 2 Gbps | minimálne 300 Mbps |
| Priepustnosť IPsec VPN | minimálne 2 Gbps | minimálne 500 Mbps |
| Max. počet súbežných spojení | minimálne 800 000 | minimálne 60 000 |
| Počet nových spojení za sekundu | minimálne 50 000 | minimálne 4 000 |
| Rozmery | maximálne 2U | maximálne 1U |
| Porty pre správu FW | minimálne 1 x 10/100/1000 out-of-band management port, 2 x 10/100/1000 high availability, 1 x 10G SFP+ high availability, 1 x RJ-45 console port, 1 x Micro USB | minimálne 1 x 10/100/1000 out-of-band management port, 1 x RJ-45 console port, 1 x Micro USB |
| Prevádzkové porty | minimálne 12 x 10/100/1000 ethernet, 4 x 1G SFP, 4 x 1G/10G SFP/SFP+ | minimálne 8 x 10/100/1000 ethernet |
| Interné úložisko | min. 200 GB SSD | min. 32 GB |

**Ďalšie požiadavky, ktoré musia ponúkané firewally typu A a typu B spĺňať:**

* Všetky parametre priepustnosti musí dodávateľ uvádzať v podmienkach reálnej prevádzky, tzv. "application mix"
* FW 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
* FW musí podporovať agregáciu portov pomocou protokolu 802.3ad (Link Aggregation Control Protocol)
* FW musí byť rozmerovo kompatibilný s 19" rozvádzačom
* FW musí podporovať dva nezávislé redundantné zdroje napájania AC 230V
* FW musí plne podporovať IPv4 aj IPv6
* FW musí podporovať zapojenie v režimoch linkovej vrstvy (s virtuálnym sieťovým rozhraním), sieťovej vrstvy, transparentný a TAP
* FW musí podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64
* FW 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
* FW musí podporovať site-to-site VPN pomocou protokolu IPSec
* FW musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS)
* Počet súčasne pripojených užívateľov nesmie byť licenčne obmedzený
* FW musí podporovať aplikačnú detekciu a kontrolu ako svoju natívnu funkcionalitu
* FW musí podporovať identifikáciu aplikácií naprieč všetkými portami / protokolmi
* Identifikácia aplikácie musí prebiehať priamo vo FW
* FW musí detegovať a zabrániť aplikácii meniť porty, tzv. Port-hopping
* FW musí podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít
* FW musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotného HW zariadenia
* FW musí podporovať dešifrovanie odchádzajúcej SSL / TLS prevádzky, za pomoci náhradného serverového certifikátu klientom
* FW musí podporovať dešifrovanie prichádzajúcej SSL / TLS prevádzky, za pomoci naimportovaného privátneho kľúča interného servera
* FW musí podporovať funkciu SSH proxy a kontrolovať tunelované aplikácie
* FW musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky
* FW 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 FW
* Aktualizácia zero-day signatúr musí byť každých minimálne 5 minút inštalovaná do FW
* FW musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - whitelisting iba povolených aplikácií a zákaz všetkého ostatného, ​​vrátane neznámej prevádzky
* FW musí obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (intrusion prevention system - IPS). Databáza IPS signatúr musí byť uložená priamo vo FW. Aplikácia IPS profilu musí byť granulárna, na úrovni bezpečnostného pravidla
* FW musí obsahovať integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr musí byť uložená priamo vo FW. Aplikácia AV profilu musí byť granulárna, na úrovni bezpečnostného pravidla
* Antivirus musí byť schopný kontrolovať prevádzku v minimálne týchto aplikáciách: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB
* FW musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa
* FW 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
* FW musia poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu
* FW 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
* FW musia 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 a pod.)
* FW musí obsahovať natívnu podporu pre využívanie databázy URL
* FW musí obsahovať lokálne úložisko záznamov
* FW musí obsahovať nástroj na analýzu záznamov bez nutnosti využitia ďalšieho systému mimo vlastného grafického používateľského prostredia
* FW musí podporovať preposielanie záznamov na zariadenia tretích strán
* FW musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov