**Opis predmetu zákazky**

Predmetom zákazky je zabezpečenie ochrany sieťovej infraštruktúry vo vybraných vzdialených lokalitách pripojených do siete MZVEZ SR. Ide o kúpu zariadení (hardvéru) – nových firewallov na účely ich integrácie do existujúceho systému centrálnej správy Palo Alto Networks Panorama, používanej verejným obstarávateľom s akceptáciou všetkých systémových nastavení, aktualizácií, politík, bezpečnostných profilov a konfigurácií NAT, prostredníctvom existujúceho systému a o kúpu podpory a licencie k hardvéru (balík služieb).

Ide o nákup nových firewallov v počte 7 kusov (z toho jeden kus ako prevádzková záloha) a 7 ks nových originálnych adaptérov k firewallom, 6 kusov služieb podpory (podpora a licencie) výrobcu vrátane poskytovania aktualizácií, bezplatnej výmeny zariadenia – firewallu pri poruche a dostupnosti technickej podpory v režime 24 hodín 7 dní v týždni, aktualizovaná ochrana pred hrozbami a filtrovanie URL adries na obdobie minimálne jeden rok. Jeden kus firewallu je určený ako prevádzková záloha pre možnosť okamžitej výmeny v prípade poruchy iného zariadenia - firewallu.

Za účelom predídenia duplicitnému zverejňovaniu dokumentov verejný obstarávateľ dáva do pozornosti uchádzačovi, že podrobné informácie o predmete zákazky sú uvedené v Technickej špecifikácii tovaru v tabuľke č. 1 „Hardvér“ a v Technickej špecifikácii tovaru „Podpora“, ktorú tvorí príloha č. 1 k časti B.1 Opis predmetu zákazky a zároveň aj zmluvy. Ide o dokument zverejnený vo formáte .docx a označená ako príloha č. 1 k zmluve, ktorá je zverejnená vo formáte .docx.

**Minimálne požiadavky na predmet zákazky**

**Technická špecifikácia tovaru „Hardvér“** Tabuľka č. 1

|  |  |
| --- | --- |
| **Minimálne požiadavky verejného obstarávateľa/ kupujúceho** | **Ponuka uchádzača/ predávajúceho** |
| HARDVÉR |
| FIREWALL  |
|  | **Typ, značka a výrobca produktu:** |
|  |
| **Technické vlastnosti** | **Hodnota/charakteristika** | **Navrhovaná hodnota/charakteristika** |
| 1. **Základné požiadavky**
 |  |
| 1.1. Bezpečnostné zariadenie typu firewall je celok zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií |  |  |
| 1.2. Výrobcom zaistená podpora minimálne po dobu plánovanej životnosti firewallu |  |  |
| 1. **Požiadavky na HW architektúru**
 |  |
| 2.1. Všetky parametre priepustnosti uvádzať v podmienkach reálnej prevádzky (real world mix pakety), tzv. "Application mix" |  |  |
| 2.2. Firewall (ďalej len "FW") typu HW appliance |  |  |
| 2.3. Modul pre spracovanie dát je v architektúre firewallu hardwarovo oddelený od ďalších podporných modulov (správa zariadenia a riadiaci modul pre podporné sieťové činnosti), aby nemohlo dôjsť k ich vzájomnému ovplyvneniu |  |  |
| 2.4. FW obsahuje jeden dedikovaný port pre správu pomocou konzoly pre prístup k CLI |  |  |
| 2.5. FW obsahuje | min. 8 metalických dátových portov s rýchlosťou prenosu 1Gbps |  |
| 2.6. FW obsahuje | min. 1 dedikovaný OOB management port pre plnohodnotnú správu FW |  |
| 2.7. Schopnosť FW ukladať zaznamenané údaje na interné úložisko s veľkosťou | min. 32 GB |  |
| 2.8. FW podporuje agregáciu portov pomocou protokolu 802.3ad (LACP) |  |  |
| 2.9. FW je rozmerovo kompatibilný s 19" rozvádzačom |  |  |
| 2.10. FW podporuje dva nezávislé redundantné zdroje napájania AC 230V |  |  |
| 1. **Všeobecné výkonové parametre**
 |
| 3.1. Hodnoty priepustnosti FW pri plnej aplikačnej kontrole dosahuje | min. 560 Mbps (app mix) |  |
| 3.2. Priepustnosť FW pri plnej aplikačnej kontrole a zapnutí všetkých dostupných signatúr IPS a AV dosahuje hodnoty | min. 260 Mbps (app mix) |  |
| 3.3. Minimálny počet súbežných spojení dosahuje hodnoty | min. 64 000 |  |
| 3.4. Minimálny počet nových spojení za sekundu dosahuje hodnoty | min. 4 200 |  |
| 1. **Sieťová funkcionalita**
 |
| 4.1. FW podporuje IPv4 aj IPv6 |  |  |
| 4.2. FW podporuje zapojenie v režimoch L2 (s virtuálnym L3 rozhraním), L3, transparent a TAP |  |  |
| 4.3. FW podporuje preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64 |  |  |
| 4.4. FW podporuje smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding) |  |  |
| 4.5. PBF umožňuje nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, používateľ |  |  |
| 1. **VPN**
 |
| 5.1. FW podporuje site-to-site VPN pomocou protokolu IPSec |  |  |
| 5.2. FW podporuje Remote Access VPN pomocou protokolov IPSec a SSL (TLS) |  |  |
| 5.3. Počet súčasne pripojených užívateľov nie je licenčne obmedzený |  |  |
| 5.4. Priepustnosť IPSec | min. 500 Mbps |  |
| 1. **Manažment**
 |
| 6.1 Jednotlivé HW zariadenie obsahuje plnohodnotné grafické rozhranie (GUI) pre správu, bez nutnosti používania centrálneho management servera. Pripojenie k GUI podporuje šifrovanie |  |  |
| 6.2. Jednotlivé HW zariadenie obsahuje plnohodnotné textové rozhranie (CLI) pre správu, bez nutnosti používania centrálneho management servera. Vzdialené pripojenie k CLI podporuje šifrovanie |  |  |
| 6.3. Jednotlivé HW zariadenie umožňuje použitie šablón pre bootstraping nových FW použitím USB flash disku |  |  |
| 6.4. FW pre autentizáciu a autorizáciu administrátorov podporuje protokoly LDAP, Radius, TACACS +, Kerberos a osobné certifikáty |  |  |
| 6.5. FW obsahuje natívny nástroj pre debugging problémových situácií v úrovni L2 - L7 ISO / OSI modelu |  |  |
| 6.6. FW podporuje natívny nástroj pre odchytenie prevádzky |  |  |
| 6.7. FW manažment podporuje prácu viac administrátorov v rovnakom čase, vrátane aplikácie politík a nastavení vytvorených iba konkrétnym administrátorom |  |  |
| 1. **Kontrola na úrovni používateľských identít**
 |
| 7.1. FW podporuje vytváranie bezpečnostných pravidiel na základe používateľských identít |  |  |
| 7.2. Voľba používateľskej identity je natívne súčasťou vytvárania štandardného bezpečnostného pravidla |  |  |
| 7.3. Užívateľská identita predstavuje "match kritérium" pri policy lookup |  |  |
| 7.4. FW podporuje získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie klienta na koncové zariadenia |  |  |
| 7.5. FW podporuje získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie klienta na doménový radič |  |  |
| 7.6. FW podporuje získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotného HW zariadenia |  |  |
| 7.7. FW podporuje získavanie väzby IP adresa-užívateľské meno z Active Directory za pomoci doménového účtu s čo najnižšími možnými právami pre čítanie Security logov, bez nutnosti disponovať rizikovými úrovňami oprávnení  |  |  |
| 7.8. FW podporuje získavanie väzby IP adresa-užívateľské meno prostredníctvom načítania informácie zo záznamu, získaného pomocou zabezpečeného protokolu Syslog |  |  |
| 7.9. FW podporuje získavanie väzby IP adresa-užívateľské meno z terminálových serverov MS (možné za pomoci nainštalovaného agenta) |  |  |
| 1. **QOS**
 |  |  |
| 8.1. FW poskytuje možnosť obmedzenia využívanej šírky pásma na základe zdrojovej a cieľovej IP adresy, portu, užívateľskej identity, aplikácie a času (od - do, deň v týždni + čas.) |  |  |
| 8.2. FW podporuje prioritizáciu prevádzky na základe DSCP |  |  |
| 8.3. FW podporuje prioritizáciu prevádzky na základe Identifikovanej aplikácie |  |  |
| 1. **Záznamy udalostí**
 |
| 9.1. FW obsahuje lokálne úložisko záznamov |  |  |
| 9.2. FW obsahuje nástroj na analýzu záznamov bez nutnosti využitia ďalšieho systému mimo GUI |  |  |
| 9.3. FW podporuje agregované zobrazenie záznamov na základe jedného filtrovacieho pravidla, naprieč jednotlivými typmi záznamov, ako sú prevádzkové záznamy, záznamy bezpečnostných incidentov a záznamy prístupov na URL |  |  |
| 9.4. FW podporuje preposielanie záznamov na zariadenia tretích strán |  |  |
| 9.5. FW umožňuje výber preposielaných záznamov na úrovni bezpečnostného pravidla |  |  |
| 9.6. Preposielané záznamy z FW sú automaticky rozpoznané používanými typmi SIEM (uvedenými v Leaders kvadrante aktuálneho Gartner MQ) |  |  |

|  |  |
| --- | --- |
| 1. **Aplikačná kontrola**
 |  |
| 10.1. FW podporuje aplikačnú detekciu a kontrolu ako svoju natívnu funkcionalitu |  |  |
| 10.2. Priradenie povolených a zakázaných aplikácií je natívne súčasťou vytvárania štandardného bezpečnostného pravidla |  |  |
| 10.3. Definovaná aplikácia predstavuje "match kritérium" pri policy lookup |  |  |
| 10.4. FW podporuje identifikáciu aplikácií naprieč všetkými portami / protokolmi |  |  |
| 10.5. FW podporuje identifikáciu aplikácií na neštandardných portoch |  |  |
| 10.6. Identifikácia aplikácie prebieha priamo vo FW |  |  |
| 10.7. FW deteguje a zabraňuje aplikácii meniť porty, tzv. Porthopping |  |  |
| 10.8. FW podporuje riadenie neznámej prevádzky |  |  |
| 10.9. FW umožňuje tvorbu užívateľsky definovaných aplikácií bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa |  |  |
| 1. **Dešifrovanie**
 |
| 11.1. FW podporuje dešifrovanie odchádzajúcej SSL / TLS prevádzky, za pomoci náhradného serverového certifikátu klientom |  |  |
| 11.2. FW podporuje dešifrovanie prichádzajúcej SSL / TLS prevádzky, za pomoci naimportovaného privátneho kľúča interného servera |  |  |
| 11.3. FW podporuje funkciu SSH proxy a kontroluje tunelované aplikácie |  |  |
| 11.4. Dekryptovanú prevádzku je možné definovať na základe URL kategórií, aj všetkých ďalších typických parametrov, ako sú zdrojová a cieľová IP adresa, port, užívateľská identita |  |  |
| 11.5. FW podporuje dešifrovanie pomocou ECC (Elliptical Curve Cryptography), vrátane DHE a ECDHE pre prichádzajúcu a odchádzajúcu prevádzku |  |  |
| 11.6. FW podporuje preposielanie dešifrovanej prevádzky na iné skenovacie zariadenie tretích strán. Zariadenie 3 strany následne prepošle čisto prefiltrované dáta späť do FW (tzv. Decryption broker). |  |  |
| 11.7. FW podporuje preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky |  |  |
| 1. **Sandboxing**
 |
| 12.1. Firewall podporuje možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom SMTP, HTTP, FTP, IMAP, POP3 a SMB |  |  |
| 12.2. Sandbox systém je od rovnakého výrobcu ako je FW, nemusí byť HW súčasťou FW |  |  |
| 12.3. Sandbox systém je schopný okamžite automaticky vytvoriť IPS / AV signatúry pre FW, v prípade, keď je testovaná vzorka vyhodnotená ako škodlivá |  |  |
| 12.4. Sandbox je schopný automaticky upraviť kategórie používanej URL databázy ak zistí, že testovaná vzorka je škodlivá a komunikuje na konkrétne URL |  |  |
| 12.5. Sandbox poskytuje aktualizácie signatúr pre AV, Webfiltering, DNS, C & C |  |  |
| 12.6. Sandbox podporuje analýzu vzorky na operačnom systéme inštalovanom priamo na hardvéri, tzn. nie vo virtuálnom prostredí |  |  |
| 12.7. Sandbox podporuje operačné systémy Windows, Linux, MacOS a Android |  |  |
| 12.8. Report z analýzy odoslanej vzorky do sandboxu je prístupný priamo z rozhrania FW |  |  |
| 12.9. Aktualizácia zero-day signatúr je každých 5 minút inštalovaná do NGFW |  |  |
| 1. **Bezpečnostné funkcionality**
 |
| 13.1. FW podporuje zavedenie tzv. pozitívneho bezpečnostného modelu - whitelisting iba povolených aplikácií a zákaz všetkého ostatného, vrátane neznámej prevádzky |  |  |
| 13.2. FW obsahuje integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (IPS). Databáza IPS signatúr je uložená priamo vo FW. Aplikácia IPS profilu je granulárna, na úrovni bezpečnostného pravidla |  |  |
| 13.3. FW umožňuje tvorbu užívateľsky definovaných IPS signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa |  |  |
| 13.4. FW obsahuje integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr je uložená priamo vo FW. Aplikácia AV profilu je granulárna, na úrovni bezpečnostného pravidla |  |  |
| 13.5. Antivírus je schopný kontrolovať prevádzku v minimálne týchto aplikáciách: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB |  |  |
| 13.6. FW umožňuje tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa |  |  |
| 13.7. FW podporuje možnosť zablokovania útoku využívajúceho známe C & C centrá aj v prípade, že je prevádzka šifrovaná a nie je možné vykonávať SSL dešifrovanie |  |  |
| 13.8. FW v bezpečnostných politikách podporuje použitie externých dynamických zoznamov |  |  |
| 13.9. FW poskytuje možnosť overiť na základe certifikátov pravosť týchto dynamických zoznamov |  |  |
| 13.10. FW pre prístup ku kritickým aplikáciám poskytuje možnosť vynútiť multifaktorové overenie prostredníctvom webového portálu, bez ohľadu na to, či cieľová aplikácia podporuje viacfaktorovú autentizáciu; táto vlastnosť je konfigurovateľná na úrovni bezpečnostného pravidla |  |  |
| 13.11. FW poskytuje možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu |  |  |
| 13.12. FW je schopný automaticky vytvárať C & C signatúry a okamžite ich aplikovať do bezpečnostnej politiky |  |  |
| 13.13. FW poskytuje funkciu ochrane proti tzv. Drive-by downloadom; spôsob ochrany musí byť pre používateľa interaktívny s možnosťou voľby akceptácie rizika a stiahnutia súboru |  |  |
| 13.14. FW podporuje analýzu DNS dotazu tzv. Sinkhole funkciou, ktorá na dotaz malware DNS URL vráti náhradnú IP adresu pre detailnejšiu analýzu a zároveň sa stanica na pôvodnú malware stránku nedostane |  |  |
| 13.15. FW poskytuje možnosť rozšírenia o funkcionalitu pokročilej analýzy DNS dotazov proti technikám používajúcim DGA (domain generation algorithm) v reálnom čase |  |  |
| 1. **Ochrana proti DoS**
 |
| 14.1. FW obsahuje natívnu službu pre ochranu proti útoku typu DoS pomocou limitácie počtu spojení na úrovni zdrojová a cieľová IP adresa, užívateľská identita a aplikácia |  |  |
| 1. **URL filtering**
 |
| 15.1. FW obsahuje natívnu podporu pre využívanie databázy URL |  |  |
| 15.2. URL databázy sú od toho istého výrobcu ako FW |  |  |
| 15.3. FW je schopný použiť URL kategóriu v definícii bezpečnostného pravidla |  |  |
| 15.4. FW podporuje vytváranie užívateľsky definovaných kategórií, bez nutnosti využiť externý nástroj a bez nutnosti zásahu výrobcu / dodávateľa |  |  |
| 15.5. URL databáza je dynamicky aktualizovaná na základe novo zistených URL, vedúcich na škodlivý obsah alebo C & C centrá |  |  |
| 15.6. URL databáza podporuje  | možnosť zaradenia do min. dvoch kategórií naraz pre jedinú URL |  |
| 15.7. Rozhranie URL databázy vo FW obsahuje možnosť požiadať o rekategorizáciu nevhodne zaradených URL bez nutnosti otvárania osobitnej požiadavky |  |  |
| 1. **Servisná podpora a licenčný plán**
 |
| 16.1. FW podporuje licenčný model nezávislý od počtu ochraňovaných koncových systémov |  |  |
| 16.2. Prevádzková náhrada umožňuje výmenu za nefunkčné zariadenie a prenesenie bezpečnostných kontraktov a podpory na toto zariadenie v prípade poruchy |  |  |
| 16.3. Zabezpečenie výmeny vadného zariadenia do dvoch pracovných dní od vrátenia vadného zariadenia. |  |  |

|  |
| --- |
| AC adaptér  |
|  | **Typ, značka a výrobca produktu:** |
|  |
| **Technické vlastnosti** | **Hodnota/charakteristika** | **Navrhovaná hodnota/charakteristika** |
| 1. Súčasťou dodávky každého firewallu je druhý originálny adaptér AC 230 V |  |  |

**Technická špecifikácia tovaru „Podpora“** Tabuľka č. 2

|  |  |
| --- | --- |
| **Minimálne požiadavky verejného obstarávateľa/ kupujúceho** | **Ponuka uchádzača/ predávajúceho** |
| PODPORA |
| Podpora výrobcu – 1 rok |
|  | **Produktový kód:** |
|  |
| **Technické vlastnosti** | **Hodnota/charakteristika** | **Navrhovaná hodnota/charakteristika** |
| 1.1. Zabezpečenie automatických aktualizácií operačného systému a bezpečnostných funkcií firewallu |  |  |

|  |  |  |
| --- | --- | --- |
| 1.2. Dostupnosť telefonickej technickej podpory a bezpečnostných expertov výrobcu v režime 24 hodín /7 dní v týždni, ktorí na základe vlastných vyšetrovacích nástrojov a postupov poskytnú pomoc pri riešení bezpečnostných udalostí, zbere záznamov a indikátorov kompromitácie |  |  |
| 1.3. Dostupnosť online portálu podpory výrobcu umožňujúcemu prístup k dokumentácii produktov, bázy dát pre riešenie prevádzkových problémov a riadenie prípadov požadovanej podpory (oznamovanie, kontrola stavu riešenia). |  |  |
| 1.4. Výmena vadného zariadenia do dvoch pracovných dní. |  |  |

|  |
| --- |
| Licencia pre funkcie ochrany pred hrozbami – 1 rok |
|  | **Produktový kód:** |
|  |
| **Technické vlastnosti** | **Hodnota/charakteristika** | **Navrhovaná hodnota/charakteristika** |
| 1. Zabezpečenie automatických aktualizácií signatúr hrozieb pre funkcie ochrany proti vírusom, spyware a zneužívaniu zraniteľností, ktoré dokáže dodaný produkt plnohodnotne spracovať a používať. |  |  |
| Licencia pre funkciu filtrovania URL adries – 1 rok |
|  | **Produktový kód:** |
|  |
| **Technické vlastnosti** | **Hodnota/charakteristika** | **Navrhovaná hodnota/charakteristika** |
| 1. Zabezpečenie automatických aktualizácií databázy pre kategorizáciu a detekciu škodlivých URL adries, ktoré dokáže dodaný produkt plnohodnotne spracovať a používať. |  |  |