1. Predmetom zákazky je zabezpečenie hardvérovej (HW) a softvérovej (SW) infraštruktúry pre rozšírenie a obmenu IaaS vládneho cloudu.
2. Verejný obstarávateľ z hľadiska opisu predmetu zákazky uvádza v súlade so zákonom č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov technické požiadavky, ktoré sa v niektorých prípadoch odvolávajú na konkrétneho výrobcu, výrobný postup, značku, patent, typ, technické normy, technické osvedčenia, technické špecifikácie, technické referenčné systémy, krajinu, oblasť alebo miesto pôvodu alebo výroby. V prípade, že by záujemca/uchádzač sa cítil dotknutý vo svojich právach, t. j., že týmto opisom by dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov/uchádzačov alebo výrobcov, alebo že tento predmet zákazky nie je opísaný dostatočne presne a zrozumiteľne, tak vo svojej ponuke môže uchádzač použiť technické riešenie ekvivalentné, ktoré spĺňa kvalitatívne, technické, funkčné požiadavky na rovnakej a vyššej úrovni, ako je uvedené v tejto časti súťažných podkladoch, túto skutočnosť však musí preukázať uchádzač vo svojej ponuke.
3. Súčasťou technických zariadení (tovarov) musí byť technická dokumentácia, obsahujúca najmä technický popis, návod na obsluhu. Technická dokumentácia je vyhotovené v slovenskom alebo v českom jazyku.
4. Kúpna cena tovarov musí zahŕňať dopravu na miesto určenia spojenú s vykládkou tovaru a likvidáciou obalov.
5. Tovar musí byť nový, nepoužívaný, zabalený v neporušených obaloch, nepoškodený. Tovar nesmie byť recyklovaný, repasovaný, renovovaný.
6. Verejný obstarávateľ si vyhradzuje právo prevziať iba tovar funkčný, bez zjavných vád, dodaný v kompletnom stave a v požadovanom množstve.   
   V opačnom prípade si vyhradzuje právo nepodpísať dodací list, neprebrať dodaný tovar a nezaplatiť cenu za neprebraný tovar.
7. Človekodeň – je merná jednotka pre vykazovanie prácnosti, za ktorú sa považuje 8 pracovných človekohodín jedného pracovníka dodávateľa, pričom Človekohodina – je merná jednotka pre vykazovanie prácnosti, za ktorú sa považuje 1 pracovná hodina (60 minút) jedného pracovníka dodávateľa.
8. **Uchádzač vo svojom vlastnom návrhu plnenia predmetu zákazky (vypracovaného podľa vzoru uvedeného v prílohe č. 1.3 SP - Opis predmetu zákazky / Vlastný návrh plnenia) uvedie: skutočnú špecifikáciu ponúkaného predmetu zákazky - výrobcu, model, technické špecifikácie, parametre a funkcionality požadované verejným obstarávateľom - uviesť áno/nie, v prípade číselnej hodnoty uviesť jej skutočnosť.**
9. **NETWORKING**

**Položka č. 1 – Sieťová karta pre existujúci agregačný smerovač a prevodníky**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** | **Vlastný návrh plnenia \*** |
| Sieťová karta pre existujúce zariadenie: | Sieťová karta pre existujúci agregačný WAN smerovač |  |
| Požadované parametre: | 1x 10GE XFP port  Kompatibilita s existujúcim zariadením Cisco ASR1000 |  |
| Počet | 4 |  |
| Prevodník | XFP 10GBase-SR |  |
| Servisná podpora: | Servisná podpora výrobcu 3 roky s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. |  |
| Počet | 4 |  |

**Položka č. 2 – Manažovateľný Layer 2 prepínač**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Požadované parametre | Verzia s 48 fixnými GigabitEthernet metalickými portami s RJ-45 konektormi  Min. 2 x 10GigabitEthernet SFP+ uplink porty s voliteľným médiom (optický multimód alebo singlemód), použiteľné aj v režime 1GE SFP Prepínacia kapacita minimálne 210 Gbps full duplex  Priepustnosť minimálne 130 Mpps Počet aktívnych VLAN min. 1023, VLAN ID 4096, unikastových MAC adries min. 16K Počet unicastových priamych smerovacích záznamov pre IPv4 a IPv6: 2K Podpora jumbo rámcov - MTU min. 9216 bajtov Napájací zdroj do napájacej siete 230V / 50Hz 512MB RAM, 128MB Flash pamäť Voliteľne rozšíriteľný o stohovací modul s priepustnosťou stohovacej zbernice 80Gbps a zapojení minimálne 8 prepínačov v stohu Manažment cez nástroj s grafickým rozhraním, alebo cez príkazový riadok, vrátane šifrovaného spojenia SSH. Podpora smerovacích protokolov – statické smerovanie a RIP Stredná doba poruchovosti MTBF v hodinách min. 350000 Podpora štandardov • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.1X • IEEE 802.1ab (LLDP) • IEEE 802.3ad |  |
| Servisná podpora: | Servisná podpora výrobcu 3 roky s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. |  |
| Počet | 2 |  |

**Položka č. 3 – Samostatné manažovateľné sieťové prepínače do existujúcej prepínacej matice a prevodníky**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Samostatné manažovateľné prepínače pracujúce na 2. a 3. vrste OSI | * vyhotovenie pre samostatné použitie s možnosťou použitia s centrálnym riadiacim systémom * priepustnosť min. 3 Tbps * 48 univerzálnych portov 1/10/25GE alebo 16/32G Fibre Channel SFP28 * min. 6 portov 40/100GE QSFP28 * podpora downlink 1/10/25 GE, 16/32 Fibre Channel * veľkosť 1RU * podpora AC napájania, redundantné zdroje * hot swap vymeniteľné zdroje aj ventilátory |  |
| Vlastnosti | * jednotný softvér (obraz) pre celý rad zariadení * jednotné konfiguračné rozhranie * dedikované rozhranie pre OOB * podpora Jumbo Frame – MTU min. 9216 bytov * zdvojenie fyzických zariadení do jedného logického celku vrátanie zdvojnásobenia výkonu (vPC) * IEEE 802.3x Flow Control * IEEE 802.3ad (LACP) * Etherchannel cez viaceré šasi * IEEE 802.1q * IEEE 802.1Qbb Priority Flow Control * IEEE 802.1d (Spanning Tree Protocol) * IEEE 802.1s MST * IEEE 802.1w RSTP * IEEE 802.1ab LLDP * IGMPv2 a IGMPv3 snooping * IGMP querier * podpora FC-FEC a RS-FEC pre porty v režime 25Gbps * podpora VXLAN BGP EVPN * možnosť podpory wire-rate MACSEC enkrypcie * lokálne aj vzdialené zrkadlenie dátových tokov, 4 relácie * podpora protokolu pre redundanciu funkcie default gateway * podpora min. RIPv2, OSPFv2, OSPFv3, PIM, IS-IS a MP BGP * podpora MSDP a Anycast-RP * podpora statického IPv4 a IPv6 smerovania * podpora policy-based smerovania * podpora DHCP Option 82 |  |
|  | * podpora MSDP a Anycast-RP * podpora statického IPv4 a IPv6 smerovania * podpora policy-based smerovania * podpora DHCP Option 82 * podpora detekcie obojsmernej prevádzky portu * hardvérová podpora prepínania unicast aj multicast IPv4 a IPv6 |  |
| Servisná podpora | Servisná podpora výrobcu 3 roky s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. |  |
| Počet | 6 |  |
| Modul optických rozhraní | SFP+ 10GBASE-SR transciever pre multimode optiku do 300m |  |
| Počet | 72 |  |
| Modul optických rozhraní | QSFP obojsmerný (BiDi) modul pre krátke vzdialenosti optického pripojenia |  |
| Počet | 64 |  |

**Položka č. 4 – Sieťová karta pre existujúci SAN prepínač a prevodníky**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Sieťová karta pre existujúce zariadenie: | Sieťová karta pre existujúci datacenter SAN FC prepínač |  |
| Požadované parametre: | 48-port 16Gbps FC Modul  Kompatibilita s existujúcim zariadením MDS 9700 |  |
| Servisná podpora | Servisná podpora výrobcu 3 roky s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. |  |
| Počet | 4 |  |
| Prevodník | 16-Gbps SW SFP+ |  |
| Počet | 64  Pozn.: Požaduje sa 64 prevodníkov, ktoré sú súčasťou 4 SAN kariet |  |

**Položka č. 5 – Modul manažmentu bezpečnosti pre existujúce bezpečnostné brány**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Modul pre existujúce riešenie: | Modul riadenia bezpečnosti pre existujúce zariadenia |  |
| Výkon | podpora min. 740 IPS snímačov |  |
| podpora min. 300 miliónov IPS eventov |  |
| minimálny výkon 20 000 fps (flows per second) |  |
| 2 x 1 Gbps RJ45, 2 x 10 Gbps SFP+ |  |
| maximálna výška 1 RU |  |
| min. 3.2 TB SSD RAID 6 |  |
| Požadované funkcionality | podpora managementu IPS režimu, Antimalvérovej ochrany, Url filtrovania pre Firewall, |  |
| podpora integrácie na SIEM |  |
| rozpoznávanie útokov od sieťovej až po aplikačnú vrstvu referenčného modelu OSI pre IPv4 aj IPv6. |  |
| podpora signatúr písaných pre Snort |  |
| rozpoznávanie operačných systémov koncových zariadení, výrobcu a typ |  |
| rozpoznávanie aplikácií na klientskych staniciach, sieťové protokoly, ako aj prihlásených používateľov. |  |
| aktivácia/deaktivácia signatúr podľa rozpoznaných OS a aplikácií a sieťovej komunikácie |  |
| aktivácia/deaktivácia signatúr s minimálnymi zásahmi zo strany obsluhy |  |
| kategorizácia útokov, upozornenie admina na zraniteľné systémy |  |
| uchovávanie histórie o prihlásených používateľoch na koncových zariadeniach v sieti |  |
| podpora registrácie min. 20 000 koncových zariadení |  |
| signatúry k dispozícii do 48 hodín od zverejnenia bezpečnostnej chyby |  |
| antimalvérová ochrana musí porovnávať signatúry s celou databázou výrobcu |  |
| zobrazenie trajektórie presunu súborov medzi koncovými zariadeniami |  |
| zobrazenie IP adries a protokolov zodpovedných za šírenie malware. |  |
| identifikácia zariadenia alebo IP adresy, odkiaľ sa začalo šírenie malware |  |
| schopnosť korelácie udalostí |  |
| definovanie korelačných politík pre automatické upozornenie administrátora |  |
| upozornenie správcu ak pripojené koncové zariadenie je v správe CnC (Command-and-Control) servera na Internete |  |
| podpora integrácie s remediačnými nástrojmi tretích strán. |  |
| Kompatibilita s a možnosť spravovania a vyhodnocovania údajov z existujúcich zariadení Cisco FirePower |  |
| Servisná podpora | 3 roky na hardvér a softvér s odozvou 8x5xNBD |  |
| Počet | 2 |  |

**Položka č. 6 – Monitoring sieťovej prevádzky so škálov 2000 Flow Rate**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Požadované funkcionality | * Virtuálna edícia monitoringu sieťovej prevádzky na báze NetFlow záznamov vygenerované virtuálnymi sondami zo sieťovej prevádzky. * Riešenie musí minimálne obsahovať jeden virtuálny management, jeden virtuálny kolektor a dve virtuálne sondy. * Riešenie by malo zaznamenávať informácie o spojeniach a tokoch v sieťovej prevádzke zo zdrojovej informácie protokolu NetFlow, ktoré je možné zobraziť cez rozhranie nezávislé od použitej platformy. Úlohou je poskytnúť užívateľovi informáciu o historickom ako i súčasnom stave siete, aktivitách v sieti a výkonnosti siete. |  |
| Servisná podpora | Prístup na servisné stránky výrobcu s možnosťou bezplatnej aktualizácie OS, firmware, minoritných a hlavných softvérových updatov, ako aj telefonická a e-mailová podpora priamo u výrobcu na obdobie 36 mesiacov. |  |
| Počet | 2 |  |

**Položka č. 7 – Bezpečnostné kontexty pre existujúce zariadenie**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Požadovaná funkcionalita | Licencia zvyšujúca maximálny počet bezpečnostných kontextov firewallu o 50  Kompatibilita s FW radu Cisco ASA 5500 |  |
| Počet | 1 |  |

**Položka č. 8 – Adaptívna bezpečnostná platforma**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Rozhrania | Min. 12x 10/100/1000 RJ-45, 4x1G SFP |  |
| 1 x RJ-45 konzolový sériový port |  |
| Podporované vlastnosti | Podpora Remote Access VPN |  |
| Podpora SSL VPN (VPN klient), Site-to-Site VPN |  |
| Rozšírenie o IPS, URL filtering a Antimalware funkcionality iba pridaním licencie |  |
| L2 funkcionality | Podpora IEEE 802.1q, 802.3ad |  |
| Podpora min. 1000 VLAN |  |
| Podpora transparentného režimu |  |
| L3 funkcionality | Podpora OSPFv2, OSPFv3, BGP, VRF |  |
| Podpora PIM-SM |  |
| Podpora IGMPv2 |  |
| Požiadavky na bezpečnosť | Podpora IKEv1 aj IKEv2 |  |
| Podpora SHA-2 (256, 384 aj 512 bitový hash) |  |
| Podpora dvojfaktorovej autentifikácie |  |
| Podpora IPSec SuiteB (RFC 6379) |  |
| Mapovanie VPN klientov do VLAN na základe skupinovej politiky |  |
| Podpora IPv6 |  |
| Podpora NAT44, NAT46, NAT64, NAT66 |  |
|  |  |
| Ochrana proti IP Spoofing |  |
| Nastavovanie parametrov jednotlivých spojení s min. podporou nasledujúcich parametrov – max počet spojení jedného klienta, max počet „embryonic“ spojení jedného klienta |  |
| Podpora TCP normalizácie, TCP intercept a randomizácie TCP sekvenčných čísiel |  |
| Filtrovanie na základe geolokácie a bezpečnostných zón |  |
| Požiadavky na IPS funkcie | Odomknutie IPS funkcií aplikovaním licencie, licencia musí byť zahrnutá v ponuke na obdobie minimálne 60 mesiacov |  |
| Podpora reputačného filtrovania IP adries a domén s možnosťou integrácie na reputačné zoznamy tretích strán |  |
| Podpora IDS aj IPS režimu |  |
| Rozpoznávanie útokov od sieťovej až po aplikačnú vrstvu referenčného modelu OSI pre IPv4 aj IPv6 |  |
| Podpora signatúr písaných pre Snort |  |
| Mapovanie signatúr na CVE (Common Vulnerabilities and Exposures) |  |
| False positive menej ako 1% |  |
| Podpora Indications of Compromise |  |
| Podpora normalizácie protokolovými dekódermi pre DNS, FTP, HTTP, SIP, IMAP, POP, SMTP, SSH a SSL |  |
| Na základe informácií o bezpečnostných slabinách operačných systémov a aplikácií rozpoznaných v sieti musí centrálny manažment navrhnúť, ktoré signatúry majú byť zapnuté, aby bolo prostredie aktívne chránené |  |
| Centrálny manažment musí rozpoznať, ktoré signatúry nie je potrebné aktivovať a ich vypnutím docieliť lepšie využitie výkonu sond pre aktívne používané signatúry |  |
| Centrálny manažment musí byť schopný kategorizovať prebiehajúce útoky tak, aby bol administrátor prednostne upozornený na útoky vedené voči zraniteľným systémom |  |
| Signatúry musia byť k dispozícii do 48 hodín od zverejnenia bezpečnostnej chyby |  |
| IPS musí chrániť prostredie od známych aj tzv. "day-zero" útokov (IPS musí analyzovať správanie sa dátových tokov, aby bolo možné detekovať aj útoky, ktoré sa bežnými mechanizmami nedetekujú) |  |
| Typy odpovedí na detekované útoky zo strany IPS sond - min. alarm do centrálneho manažmentu, ukončenie spojenia, zahadzovanie paketov, ukladanie obsahu paketov, interaktívna HTTP odpoveď |  |
| Manažment musí umožniť definovanie korelačných politík pre automatické upozornenie administrátora IPS, že sa útočník snaží zneužiť bezpečnostnú dieru v systéme, ktorú ešte správca napadnutého systému nestihol zaplátať. Manažment musí upozorniť správcu aj v prípade, že pripojené koncové zariadenie je v správe CnC (Command-and-Control) servera v Internete |  |
| Výsledkom korelačnej politiky je min. Syslog, email a NMAP sken. Manažment musí podporovať integráciu s remediačnými nástrojmi tretích strán |  |
| Podpora vlastných IPS signatúr |  |
| V prípade rozšírenia o antimalvér fukcionalitu, musí antimalvér vzorky porovnávať s celou databázou výrobcu |  |
| Výkon | Firewall priepustnosť : min. 2,5 Gbps |  |
| Počet súčasných spojení : min. 1 000 000 |  |
| Podporovaný počet nových spojení za sekundu: min. 14 000 |  |
| Priepustnosť TLS: min. 350 Mbps |  |
| Priepustnosť IPSEC VPN: min. 2.5 Gbps |  |
|  |  |
| Napájanie | AC napájací zdroj |  |
| Fyzické vlastnosti | Montovateľný do 19 palcového racku |  |
|  | Výška max. 1 RU |  |
| Servisná podpora | Prístup na servisné stránky výrobcu s možnosťou bezplatnej aktualizácie OS, firmware, minoritných a hlavných softvérových updatov, ako aj telefonická a e-mailová podpora priamo u výrobcu v rozsahu s odozvou 8x5xNBD na obdobie 36 mesiacov. |  |
| Počet zariadení | Riešenie musí pozostávať z 2 redundantných zariadení v clustri. |  |

1. **SECURITY**

**Položka č. 1 – Modul do existujúceho šasi pre riadenie bezpečnosti a aplikácií a prevodníky**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Blade modul | Blade modul pre existujúce blade šasi |  |
| Blade výkon | Umožní navýšenie maximálneho počtu o 20 kontextov pre celé šasi. Schopnosť spracovať:  min. 2 milióny L7 požiadaviek za sekundu  min. 1 milióny L4 spojení za sekundu  min. 14 miliónov L4 HTTPS požiadaviek za sekundu  min. 48 miliónov spojení súčasne  min. 80 Gbps L7/L4 priepustnosť  min. 200 000 SSL transakcií za sekundu (1K kľúče, RC4-MD5)  min. 44 000 SSL transakcií za sekundu (2K kľúče)  min. 10 mil. súbežných SSL spojení  Kompatibilita s existujúcim šasi Viprion 2400  Min. 4 QSFP+ sloty |  |
| Servisná podpora: | Servisná podpora na 3 roky od výrobcu s výmenou zariadenia v prípade poruchy nasledovný pracovný deň počas nahlásenia v režime 24x7. |  |
| Počet modulov | 2 |  |
| Počet prevodníkov | 4 |  |
| Licencia: | Licencia pre softvérový modul ASM, ktorá rozšíri momentálnu licenciu na celom šasi. Tento modul umožní používanie Web Application Firewall, ktorý poskytuje zabezpečenie na aplikačnej úrovni. |  |
| Počet Licencií | 1 |  |

**Položka č. 2 – Privilegovaný prístup administrátorov**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Manažovací server pre monitoring a riadenie privilegovaných prístupov | Manažovací server umožňuje riadenie a monitorovanie manažmentových relácií administrátorov, cez ktoré spravujú zariadenia vo svojich projektoch (RDP, SSH).   * Relácie je možné nahrávať a archivovať pre účely forenznej analýzy. * Okrem obrazového záznamu server ukladá aj metadáta a logy. * Súčasťou riešenia je databáza, do ktorej sú dáta ukladané. * Podpora multifaktorového overenia administrátorov * Riešenie obsahuje úložisko prihlasovacích údajov s možnosťou ich automatizovaného manažmentu a rotácie hesiel pomocou nastavených politík. * Každý tenant má samostatný manažovací PAM server minimálne pre protokoly SSH, RDP, HTTPS a SC , aby bola zaistená dôvernosť v rámci jeho projektu bez prístupu tretích strán k tenantovým reláciam, účtom, heslám a prostredníctom nich k spravovaným zariadeniam. * Počet súbežných relácií a počet súbežných používateľov nemá byť licenčne obmedzený. * Ovládanie pomocou REST API. |  |
| Servisná podpora: | Podpora pre appliancie manažovacieho servera s dĺžkou trvania 3 roky, prípadne príslušný počet ročných licencií spojených do dĺžky trvania 3 roky. |  |
| Počet licencií | Licencie pre 4000 administrátorov  Neobmedzený počet spravovaných zariadení  Všetky potrebné licencie (OS a pod.) pre beh centrálnej časti riešenia |  |

1. **NETWORKING a SECURITY**

**Položka č. 1 – Inštalačné a konfiguračné práce – hardvér**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Inštalačné a konfiguračné  práce | Tvorba dizajnu rozmiestnenia zariadení do rack-ov a zapojenia kabeláže  Úprava IP adresného plánu  Tvorba testovacích procedúr  Fyzická inštalácia zariadení do rack-ov  Zapojenie a označenie napájacej kabeláže  Zapojenie a označenie dátovej kabeláže  Spustenie zariadení a kontrola funkčnosti jednotlivých zariadení  Technická a prevádzková dokumentácia IKT infraštruktúry |  |
| Počet človekodní | 668 |  |

**Položka č. 2 - Inštalačné a konfiguračné práce – softvér**

|  |  |  |
| --- | --- | --- |
| **Produkt/Parameter** | **Požiadavky** |  |
| Inštalačné a konfiguračné  práce | Aktualizácia softvéru zariadení  Konfigurácia zariadení Firewall v súlade s dizajnom sieťovej infraštruktúry  Konfigurácia zariadení Loadbalancer v súlade s dizajnom sieťovej infraštruktúry  Konfigurácia zariadení monitorujúcich sieťové anomálie v súlade s dizajnom sieťovej infraštruktúry  Konfigurácia zariadení systému riadenia prístupov v súlade s dizajnom sieťovej infraštruktúry  Technická a prevádzková dokumentácia IKT infraštruktúry  Realizácia migrácie/upgrade virtuálnej farmy |  |
| Počet človekodní | 563 |  |