Príloha č. 1 k časti B. *OPIS PREDMETU ZÁKAZKY*

Podrobný opis predmetu zákazky

1. Požiadavky na dodávku sieťových zariadení
   1. Predmetom dodania sú, čo množstva, druhu a rozsahu sieťové zariadenia uvedené v tabuľkách č. 2, č. 4 , č. 6, č. 8 a č. 10.
   2. Uchádzač sa zaväzuje, že všetky dodané sieťové zariadenia budú nové, nerepasované, nepoužívané a od jedného výrobcu jednej značky, jedna verzia OS na všetkých dodaných zariadeniach.
   3. Všetky dodané sieťové zariadenia a súvisiace komponenty (všetok inštalačný materiál potrebný k naplneniu diela, napr. napájacie káble, optické moduly, úchyty do rackov, atď.) musia byť originálne produkty, dodané cez autorizovaných distribučných partnerov.
   4. Uchádzač sa zaväzuje, že všetky dodané sieťové zariadenia budú výrobcom podporované minimálne 60 mesiacov od odoslania ponuky.
   5. Úspešný uchádzač je povinný v termíne do 14 dní od nadobudnutia účinnosti zmluvy doručiť písomne v listinnej podobe verejnému obstarávateľovi doklad od výrobcu dodávaných sieťových zariadení, že žiadne z dodaných sieťových zariadení produktov nebudú minimálne 60 mesiacov EOS (End of Support).
   6. Uchádzač je povinný určiť celkovú cenu tak, aby zahŕňala všetky a akékoľvek náklady (doprava tovaru do miesta plnenia, náklady na odstraňovanie chýb počas záručnej doby, atď.) spojené s plnením zmluvy.
   7. Verejný obstarávateľ požaduje, aby dodané sieťové zariadenia spĺňali hardvérové a softvérové požiadavky uvedené v nasledujúcich tabuľkách č. 1, č. 3, č. 5., č. 7 a č. 9.

*Tabuľka č. 1: Sieťový prepínač typ 1 - technická špecifikácia*

|  |  |  |
| --- | --- | --- |
| **Poradové číslo** | **Sieťový prepínač typ 1 - technická špecifikácia** | **Spôsob naplnenia požiadavky s odkazom do dokumentácie** |
| --- | ***Sieťové rozhrania:*** | *---* |
| 1 | 1GE/10GE SFP+ min 48x | *<vyplní uchádzač>* |
| 2 | 100GE QSFP28 min 4x | *<vyplní uchádzač>* |
| 3 | 40GE QSFP+ min 6x |  |
| 4 | Dedikovaný MNG port min 1x RJ45 min 1GE | *<vyplní uchádzač>* |
| 5 | Console port (CLI) min 1x RJ45 | *<vyplní uchádzač>* |
| --- | ***Parametre sieťového prepínača*** | *---* |
| 6 | Minimálna prepínacia kapacita (Duplex) 1760 Gbps | *<vyplní uchádzač>* |
| 7 | Minimálne spracovanie počtu paketov za sekundu 1518 Mpps | *<vyplní uchádzač>* |
| 8 | Latencia <= 800 ns |  |
| 9 | MAC addresses Storage min 144.000 | *<vyplní uchádzač>* |
| 10 | VLANs min 4 000 | *<vyplní uchádzač>* |
| 11 | Smer prúdenia a odvod vzduchu zo strany do zadu (side-to-back) alebo spredu dozadu | *<vyplní uchádzač>* |
| 12 | Prevedenie Rack mount 1U, kompletné príslušenstvo pre montáž do racku súčasťou | *<vyplní uchádzač>* |
| 13 | Podpora min. nasledovných funkcionalít: Jumbo Frame, DHCP Relay, DHCP snooping , RBAC , QoS 802.1p, 802.3ad Link Aggregation, 802.1q VLAN tagging , 802.1q VLAN tagging , | *<vyplní uchádzač>* |
| 14 | Podpora min.: STP, RSTP, MSTP vrýtane rozšírenia BPDU guard, Root guard, Loop guard , Zrkadlenie sieťových rozhraní , Podpora SNMP a syslog , Port Mirroring | *<vyplní uchádzač>* |
| 15 | Podpora min.: IEEE 802.1ab LLDP-MED, IEEE 802.1X Authentication Port-based, IEEE 802.1X Authentication MAC-based, IEEE 802.1X Guest and Fallback VLAN, IEEE 802.1X MAC Access Bypass (MAB), IEEE 802.1X Dynamic VLAN Assignment, IEEE 802.1X open auth, IEEE 802.1X EAP pass-through, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, IEEE 802.1ae MAC Security (MAC Sec), IEEE 802.1p Based Priority Queuing | *<vyplní uchádzač>* |
| 16 | Podpora min.: Radius CoA (Change of Authority), Radius Accounting, MAC-IP Binding, sFlow, Flow Export - NetFlow v9 and IPFIX, ACL | *<vyplní uchádzač>* |
| 17 | Podpora min.: DHCP-Snooping, Dynamic ARP Inspection, IP source guard, Sticky MAC and MAC Limit, Per-port and per-VLAN MAC learning limit, Assign VLANs via Radius attributes (RFC 4675), DHCP Relay Agent Information Option, CoS based (Ethernet) a CoS tag (802.1Q frames frames), | *<vyplní uchádzač>* |
| 18 | Podpora min.: IP TOS/DSCP Based Priority Queuing, Explicit Congestion Notification, Egress priority tagging, DSCP-based a IP precedence CoS , SSH a HTTPS management, | *<vyplní uchádzač>* |
| 19 | QoS klasifikácia a markovanie na základe ACL (IP) - src/dst IP adresa, src/dst port, protocol | *<vyplní uchádzač>* |
| 20 | Podpora REST API pre konfiguráciu a monitorovanie prvkov | *<vyplní uchádzač>* |
| 21 | Podpora spájania zariadení do logického celku | *<vyplní uchádzač>* |
| 22 | Security extended from NGFW | *<vyplní uchádzač>* |
| 23 | Redundantné napájacie zdroje AC | *<vyplní uchádzač>* |
| 24 | Prepínače musia byť plne integrovateľné s existujúcou firewall platformou (FG-1801F) ako na funkčnej, tak na riadiacej úrovni. | *<vyplní uchádzač>* |
| --- | ***Minimálne požiadavky na funkčnú integráciu:*** | *---* |
| 25 | Jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu FortiManager | *<vyplní uchádzač>* |
| 26 | Vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používateľa (firewally, prepínače, Wireless Prístupové body, koncové stanice/užívatelia) | *<vyplní uchádzač>* |
| 27 | Sieťové prepínače musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice | *<vyplní uchádzač>* |
| 28 | Možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno | *<vyplní uchádzač>* |
| 29 | Vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií | *<vyplní uchádzač>* |
| 30 | Možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme | *<vyplní uchádzač>* |
| 31 | Vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia | *<vyplní uchádzač>* |
| 32 | Integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo identity používateľa | *<vyplní uchádzač>* |
| 33 | Sieťové prepínače musia podporovať funkcionality Zero trust Network Access (ZTNA) prístup a musia byť kompatibilné s existujúcim centrálnym ZTNA riešením od spoločnosti Fortinet prevádzkovaným verejným obstarávateľom. | *<vyplní uchádzač>* |
| 34 | Podpora kontroly prístupu do siete na základe bezpečnostných TAG-ov vydávaných existujúcim centrálnym ZTNA riešením pre každého používateľa. | *<vyplní uchádzač>* |
| 35 | Podpora riadenia prístupu tzv. mikrosegmentácia na základe bezpečnostných TAG-ov vydávaných existujúcim centrálnym ZTNA riešením pre každého používateľa. | *<vyplní uchádzač>* |
| 36 | Možnosť hromadnej aktualizácie (upgrade) OS prepínačov z centrálnej konzoly FortiManager. | *<vyplní uchádzač>* |
| 37 | Možnosť konfigurácie a následnej správy dodaných sieťových zariadení prostredníctvom existujúceho manažmentového nástroja FortiManager. | *<vyplní uchádzač>* |
| 38 | V prípade, že pre požadované funkcionality v tejto tabuľke sú potrebné licencie, tieto licencie musia byť súčasťou cenovej ponuky na obdobie 5 rokov | *<vyplní uchádzač>* |
| 39 | Nastavenie integrácie s riešením Progress Flowmon, t.j. minimálne posielanie flow dát vo formáte a spôsobom ktorý Progress Flowmon pre danú technológiu podporuje. | *<vyplní uchádzač>* |

*Tabuľka č. 2: Sieťový prepínač typ 1 - počet kusov*

|  |  |  |
| --- | --- | --- |
| **Položka** | **Názov produktu** | **Počet ks** |
| 1 | Sieťový prepínač typ 1 | 2 |
| 2 | Podpora výrobcu pre sieťový prepínač typ 1 na 60 mesiacov | 2 |

*Tabuľka č. 3: Sieťový prepínač typ 2 - technická špecifikácia*

|  |  |  |
| --- | --- | --- |
| **Poradové číslo** | **Sieťový prepínač typ 2 - technická špecifikácia** | **Spôsob naplnenia požiadavky s odkazom do dokumentácie** |
| --- | ***Sieťové rozhrania:*** | *---* |
| 1 | 1GE RJ45 s podporov PoE 802.3af/at min 48x | *<vyplní uchádzač>* |
| 2 | 1/10 GE SFP+ min 4x | *<vyplní uchádzač>* |
| 3 | Dedikovaný MNG port min 1x RJ45 min 1GE | *<vyplní uchádzač>* |
| 4 | Console port (CLI) min 1x RJ45 | *<vyplní uchádzač>* |
| --- | ***Parametre sieťového prepínača:*** | *---* |
| 5 | Minimálna prepínacia kapacita (Duplex) 176 Gbps | *<vyplní uchádzač>* |
| 6 | Minimálne spracovanie počtu paketov za sekundu 262 Mpps | *<vyplní uchádzač>* |
| 7 | Latencia <= 1μs |  |
| 8 | MAC addresses Storage min 32 000 | *<vyplní uchádzač>* |
| 9 | VLANs min 4 000 | *<vyplní uchádzač>* |
| 10 | Smer prúdenia a odvod vzduchu zo strany do zadu (side-to-back) alebo spredu dozadu | *<vyplní uchádzač>* |
| 11 | Prevedenie Rack mount 1U, kompletné príslušenstvo pre montáž do racku súčasťou | *<vyplní uchádzač>* |
| 12 | Minimálny PoE výkon 772 W | *<vyplní uchádzač>* |
| 13 | Podpora min. nasledovných funkcionalít: Jumbo Frame, DHCP Relay, DHCP snooping , RBAC , QoS 802.1p, 802.3ad Link Aggregation, 802.1q VLAN tagging , 802.1q VLAN tagging , | *<vyplní uchádzač>* |
| 14 | Podpora min.: STP, RSTP, MSTP vrýtane rozšírenia BPDU guard, Root guard, Loop guard , Zrkadlenie sieťových rozhraní , Podpora SNMP a syslog , Port Mirroring | *<vyplní uchádzač>* |
| 15 | Podpora min.: IEEE 802.1ab LLDP-MED, IEEE 802.1X Authentication Port-based, IEEE 802.1X Authentication MAC-based, IEEE 802.1X Guest and Fallback VLAN, IEEE 802.1X MAC Access Bypass (MAB), IEEE 802.1X Dynamic VLAN Assignment, IEEE 802.1X open auth, IEEE 802.1X EAP pass-through, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, IEEE 802.1ae MAC Security (MAC Sec), IEEE 802.1p Based Priority Queuing | *<vyplní uchádzač>* |
| 16 | Podpora min.: Radius CoA (Change of Authority), Radius Accounting, MAC-IP Binding, sFlow, Flow Export - NetFlow v9 and IPFIX, ACL | *<vyplní uchádzač>* |
| 17 | Podpora min.: DHCP-Snooping, Dynamic ARP Inspection, IP source guard, Sticky MAC and MAC Limit, Per-port and per-VLAN MAC learning limit, Assign VLANs via Radius attributes (RFC 4675), DHCP Relay Agent Information Option, CoS based (Ethernet) a CoS tag (802.1Q frames frames) | *<vyplní uchádzač>* |
| 18 | Podpora min.: IP TOS/DSCP Based Priority Queuing, Explicit Congestion Notification, Egress priority tagging, DSCP-based a IP precedence CoS , SSH a HTTPS management | *<vyplní uchádzač>* |
| 19 | QoS klasifikácia a markovanie na základe ACL (IP) - src/dst IP adresa, src/dst port, protocol | *<vyplní uchádzač>* |
| 20 | Podpora REST API pre konfiguráciu a monitorovanie prvkov | *<vyplní uchádzač>* |
| 21 | Podpora spájania zariadení do logického celku | *<vyplní uchádzač>* |
| 22 | Security extended from NGFW | *<vyplní uchádzač>* |
| 23 | Redundantné napájacie zdroje AC | *<vyplní uchádzač>* |
| 24 | Prepínače musia byť plne integrovateľné s existujúcou firewall platformou (FG-1801F) prevádzkovanou verejným obstarávateľom, ako na funkčnej, tak na riadiacej úrovni | *<vyplní uchádzač>* |
| --- | ***Minimálne požiadavky na funkčnú integráciu:*** | *---* |
| 25 | Jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu FortiManager. | *<vyplní uchádzač>* |
| 26 | Vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používateľa (firewally, prepínače, Wireless Prístupové body, koncové stanice/užívatelia) | *<vyplní uchádzač>* |
| 27 | Koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice | *<vyplní uchádzač>* |
| 28 | Možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno | *<vyplní uchádzač>* |
| 29 | Vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií | *<vyplní uchádzač>* |
| 30 | Možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme | *<vyplní uchádzač>* |
| 31 | Vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia | *<vyplní uchádzač>* |
| 32 | Integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo identity používateľa | *<vyplní uchádzač>* |
| 33 | Zariadenia musia podporovať funkcionality Zero trust Network Access (ZTNA) prístup a musia byť kompatibilné s existujúcim centrálnym ZTNA riešením od spoločnosti Fortinet prevádzkovaným verejným obstarávateľom | *<vyplní uchádzač>* |
| 34 | Podpora kontroly prístupu do siete na základe bezpečnostných TAG-ov vydávaných existujúcim centrálnym ZTNA riešením pre každého používateľa | *<vyplní uchádzač>* |
| 35 | Podpora riadenia prístupu tzv. mikrosegmentácia na základe bezpečnostných TAG-ov vydávaných existujúcim centrálnym ZTNA riešením pre každého používateľa. | *<vyplní uchádzač>* |
| 36 | Možnosť hromadnej aktualizácie (upgrade) OS prepínačov z centrálnej konzoly FortiManager. | *<vyplní uchádzač>* |
| 37 | Možnosť konfigurácie a následnej správy dodaných zariadení prostredníctvom existujúceho manažmentového nástroja FortiManager. | *<vyplní uchádzač>* |
| 38 | V prípade, že pre požadované funkcionality v tejto tabuľke sú potrebné licencie budú tieto licencie súčasťou cenovej ponuky na obdobie 5 rokov | *<vyplní uchádzač>* |
| 39 | Nastavenie integrácie s riešením Progress Flowmon, t. j. minimálne posielanie flow dát vo formáte a spôsobom ktorý Progress Flowmon pre danú technológiu podporuje. | *<vyplní uchádzač>* |

*Tabuľka č. 4: Sieťový prepínač typ 2 - počet kusov*

|  |  |  |
| --- | --- | --- |
| **Položka** | **Názov produktu** | **Počet ks** |
| 1 | Sieťový prepínač typ 2 | 130 |
| 2 | Podpora výrobcu pre sieťový prepínač typ 2 na 60 mesiacov | 130 |

*Tabuľka č. 5: Sieťový smerovač typ 1 - technická špecifikácia*

|  |  |  |
| --- | --- | --- |
| **Poradové číslo** | **Sieťový smerovač typ 1 - technická špecifikácia** | **Spôsob naplnenia požiadavky s odkazom do dokumentácie** |
| --- | **Sieťové rozhrania:** | *---* |
| 1 | 1GE RJ45 min 16x | *<vyplní uchádzač>* |
| 2 | 1 GE SFP min 8x | *<vyplní uchádzač>* |
| 3 | 10 GE SFP+ min 4x | *<vyplní uchádzač>* |
| 4 | Dedikovaný MNG port min 1x RJ45 min 1GE | *<vyplní uchádzač>* |
| 5 | Dedikovaný HA port min 1x RJ45 min 1GE | *<vyplní uchádzač>* |
| 6 | Console port (CLI) min 1x RJ45 | *<vyplní uchádzač>* |
| --- | **Parametre pre networking a firewalling:** | *---* |
| 7 | Next Generation Firewall (NGFW) | *<vyplní uchádzač>* |
| 8 | Priepustnost Firewall pre IPv4 minimálne 39/39/28 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B) | *<vyplní uchádzač>* |
| 9 | Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním minimálne 5 Gbps | *<vyplní uchádzač>* |
| 10 | Firewall Throughput (packet per second - počet spracovaných paketov za 1 sekundu) minimálne 40000000 | *<vyplní uchádzač>* |
| 11 | Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním min 3 Gbps | *<vyplní uchádzač>* |
| 12 | Počet súčasných TCP spojení firewallu - Concurrent Sessions (TCP) minimálne 3 Milion | *<vyplní uchádzač>* |
| 13 | Počet nových TCP spojení za sekundu (setup-rate) minimálne 140 000 | *<vyplní uchádzač* |
| 14 | Latencia firewallu maximálne 4 μs (merané na malých UDP paketoch (64B)) | *<vyplní uchádzač* |
| 15 | Firewall policies minimálne 8 000 | *<vyplní uchádzač>* |
| 16 | Priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response) minimálne 6 Gbps | *<vyplní uchádzač>* |
| 17 | Priepustnosť funkcie IPS min 5 Gbps | *<vyplní uchádzač>* |
| 18 | Priepustnosť SSL dešifrovania/SSL inšpekcie minimálne 3 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou) | *<vyplní uchádzač>* |
| 19 | Funkcia detekcie aplikácií na L7 (Application Control) | *<vyplní uchádzač>* |
| 20 | Podpora SSL VPN | *<vyplní uchádzač>* |
| 21 | Podpora TLS verzie 1.3 | *<vyplní uchádzač>* |
| 22 | Priepustnosť SSL VPN minimálne 1.5Gbps | *<vyplní uchádzač>* |
| 23 | Priepustnosť IPSEC VPN (512 byte) min 35 Gbps |  |
| 24 | Podpora IPSEC VPN v režime site-2-site aj client-2-site | *<vyplní uchádzač>* |
| 25 | Podpora minimálne 10 izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod. Ak je pre túto funkcionalitu potrebná licencia, súčasťou ponuky musí byť pokryté minimálne 5 kontextov. | *<vyplní uchádzač>* |
| 26 | Podpora minimálne 4000 VLAN | *<vyplní uchádzač>* |
| 27 | Podpora LACP | *<vyplní uchádzač>* |
| 28 | Podpora statických ale aj dynamických smerovacích protokolov minimálne BGP, OSPF ( potrebné licencie súčasťou dodávky) | *<vyplní uchádzač>* |
| 29 | Podpora integrácie na MS Active directory pre potreby riadenia prístupov ACL na základe identít AD (napr. Username, computer, …) potrebné licencie súčasťou dodávky | *<vyplní uchádzač>* |
| 30 | Podpora funkcie transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri ( potrebné licencie súčasťou dodávky) | *<vyplní uchádzač>* |
| 31 | Podpora protokolu FortiLink pre integráciu s Forti switchom | *<vyplní uchádzač>* |
| 32 | Deployment and management via FortiManager | *<vyplní uchádzač>* |
| --- | ***Ostatné požiadavky:*** | *---* |
| 33 | HW appliance NGFW/UTM firewall; Platforma postavená na HW akcelerovanej architektúre (t. j. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií. | *<vyplní uchádzač>* |
| 34 | Interné úložisko pre logy a konfigurácie minimálne 480 GB SSD | *<vyplní uchádzač>* |
| 35 | Požiadavky na chladenie (nasávanie-vyfukovanie) z boku do zadu alebo spredu dozadu | *<vyplní uchádzač>* |
| 36 | Prevedenie HW appliance do racku s veľkosťou 1RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu; Zariadenie vybavené dvoma zdrojmi; | *<vyplní uchádzač>* |
| 37 | Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky. | *<vyplní uchádzač>* |
| 38 | Požiadavky na funkčnosť - FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu | *<vyplní uchádzač>* |
| 39 | Požiadavky na funkčnosť - Podpora SNMP vrátane SNMP MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete (Zabbix). Požadovaná verzia minimálne SNMPv3. | *<vyplní uchádzač>* |
| 40 | Požiadavky na funkčnosť - Detekcia známych aplikácií na základe signatúr, min 3500 preddefinovaných aplikácií/signatúr. Aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu. | *<vyplní uchádzač>* |
| 41 | Požiadavky na funkčnosť - Možnosť definície FW pravidel v tzv. NGFW režime (t. j. súčasťou základnej definície FW pravidla) je: minimálne zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo. | *<vyplní uchádzač>* |
| 42 | Požiadavky na funkčnosť - podpora použitia Application control aj formou profilov priradených k pravidlám | *<vyplní uchádzač>* |
| 43 | Požiadavky na funkčnosť - Podpora funkcie DNS filtra. Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii, možnosť definovať vlastný tzv. blacklist domén, možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL. | *<vyplní uchádzač>* |
| 44 | Požiadavky na funkčnosť - Pre populárne cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii). Aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu | *<vyplní uchádzač>* |
| 45 | Požiadavky na funkčnosť - možnosť definície FW pravidel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je minimálne zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo. | *<vyplní uchádzač>* |
| 46 | Požiadavky na funkčnosť - Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos | *<vyplní uchádzač>* |
| 47 | Požiadavky na funkčnosť - Funkcie detekcie a zamedzenia narušení (IPS/IDS), funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám | *<vyplní uchádzač>* |
| 48 | Požiadavky na funkčnosť - možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS | *<vyplní uchádzač>* |
| 49 | Požiadavky na funkčnosť - Funkcie antivírovej kontroly, Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom. Ak funkcie vyžadujú licenciu, tak táto musí byť súčasťou dodávky. | *<vyplní uchádzač>* |
| 50 | Požiadavky na funkčnosť - podpora AV kontroly o rozšírenie o inšpekciu tzv. sandbox technikou. Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky | *<vyplní uchádzač>* |
| 51 | Požiadavky na funkčnosť - Podpora služby výrobcu umožňujúca detekovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej sa aktualizujúcej databázy hash-ov | *<vyplní uchádzač>* |
| 52 | Požiadavky na funkčnosť - Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky | *<vyplní uchádzač>* |
| 53 | Požiadavky na funkčnosť - Možnosť kombinovať akcie pre automatizačné pravidlá, minimálne webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy. | *<vyplní uchádzač>* |
| 54 | Požiadavky na funkčnosť - Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel, min. schopnosť parsovat vstupy z logov a z predchádzajúcich vykonaných akcií | *<vyplní uchádzač>* |
| 55 | Požiadavky na funkčnosť - Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať. | *<vyplní uchádzač>* |
| 56 | Podpora otvoreného API pre ďalšie možnosti integrácie | *<vyplní uchádzač>* |
| 57 | Natívna podpora SD-WAN funkcionality ktorá je požadovaná ako súčasť dodávaného zariadenia aj s potrebnými licenciami a ktorú je možné konfigurovať a následne spravovať prostredníctvom existujúceho manažmentového nástroja. | *<vyplní uchádzač>* |
| 58 | Zariadenia musia podporovať funkcionality Zero trust Network Access (ZTNA) prístup a musia byť kompatibilné s existujúcim centrálnym ZTNA riešením od spolocnosti Fortinet prevádzkovaným verejným obstarávateľom | *<vyplní uchádzač>* |
| 59 | Požiadavky na funkčnosť - Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky bez nutnosti samostatnej inštalácie politík. FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu. Konfigurácia a plnohodnotná následná správa dodaných zariadení prostredníctvom existujúceho manažmentového nástroja FortiManager prevádzkovaným verejným obstarávateľom | *<vyplní uchádzač>* |
| 60 | Nastavenie integrácie s riešením Progress Flowmon , t. j. minimálne posielanie flow dát vo formáte a spôsobom ktorý Progress Flowmon pre danú technológiu podporuje. | *<vyplní uchádzač>* |

*Tabuľka 6: Sieťový smerovač typ 1 - počet kusov*

|  |  |  |
| --- | --- | --- |
| **Položka** | **Názov produktu** | **Počet ks** |
| 1 | Sieťový smerovač typ 1 | 28 |
| 2 | Podpora výrobcu pre sieťový smerovač typ 1 na 60 mesiacov | 28 |

*Tabuľka č. 7: Sieťový modul typ 1 - technická špecifikácia*

|  |  |  |
| --- | --- | --- |
| **Poradové číslo** | **Sieťový modul typ 1 - technická špecifikácia** | **Spôsob naplnenia požiadavky s odkazom do dokumentácie** |
| --- | **TRAN-QSFP+SR** | *---* |
| 1 | 40GE QSFP+ | <vyplní uchádzač> |
| 2 | optický multimod duplex modul, rýchlosti min. 40 Gbps | <vyplní uchádzač> |
| 3 | transceiver module, short range for system with QSFP+ Slots | <vyplní uchádzač> |
| 4 | transciever kompatibilný s dodávanými zariadeniami | <vyplní uchádzač> |

*Tabuľka 8: Sieťový modul typ 1 - počet kusov*

|  |  |  |
| --- | --- | --- |
| **Položka** | **Názov produktu** | **Počet ks** |
| 1 | Sieťový modul typ 1 | 16 |

*Tabuľka č. 9: Sieťový modul typ 2 - technická špecifikácia*

|  |  |  |
| --- | --- | --- |
| **Poradové číslo** | **Sieťový modul typ 2 - technická špecifikácia** | **Spôsob naplnenia požiadavky s odkazom do dokumentácie** |
| --- | **SFP+modul 10Gbps** | *---* |
| 1 | FN-TRAN-SFP+SR | <vyplní uchádzač> |
| 2 | optický multimod duplex modul, rýchlosti min. 10 Gbps | <vyplní uchádzač> |
| 3 | transciever kompatibilný s dodávanými zariadeniami | <vyplní uchádzač> |

*Tabuľka 10: Sieťový modul typ 2 - počet kusov*

|  |  |  |
| --- | --- | --- |
| **Položka** | **Názov produktu** | **Počet ks** |
| 1 | Sieťový modul typ 2 | 330 |

1. Požiadavky na vykonanie inštalačných a konfiguračných prác pre dodávané sieťové zariadenia
   1. Verejný obstarávateľ požaduje vykonanie inštalačných a konfiguračných prác vo forme inštalácie na dodávané zariadenia. Minimálny rozsah inštalačných prác je uvedený v nasledujúcej tabuľke č. 11.

*Tabuľka č. 11 – Požadované inštalačné práce*

|  |  |  |
| --- | --- | --- |
| **Poradové číslo** | | **Popis** |
|  | 1 | Návrh dizajnu implementácie modernizácie LAN v spolupráci s verejným obstarávateľom |
|  | 2 | HLD – high level design, definícia pobočiek, definícia prepojenia jednotlivých pobočiek, príprava nákresov zapojenia pobočiek a ich integrácia do existujúcej infraštruktúry |
|  | 3 | LLD – low level design. Príprava IP adresácie pre manažment dodávaných zariadení. |
|  | 4 | LLD - Návrh L3 prepojení medzi jednotlivými pobočkami, návrh routingu na týchto prepojeniach. Je požadované využiť dynamický routovaci protokol (BGP alebo OSPF). |
|  | 5 | LLD – Návrh zónovania pripojených užívateľov a služieb na jednotlivých pobočkách. Návrh segmentácie siete na pobočkách na úrovni L2 – definícia jednotlivých vlan aj na úrovni L3 – návrh IP subnetov pre jednotlivé skupiny pripojených zariadení a užívateľov |
|  | 6 | LLD – definovanie prístupových politík pre pripájané zariadenia, tzv. NAC – network access control |
|  | 7 | LLD – zakreslenie detailného návrhu pripojenia pobočiek aj pobočiek samotných |
|  | 8 | Uchádzač vykoná analýzu dátových tokov od používateľov smerom na serverovú infraštruktúru a navrhne všetky potrebné FW pravidlá. Jedná sa cca o 1000 používateľov a do 300 cieľových systémov. |
|  | 9 | Sieťové nastavenie, konfigurácia administrátorských účtov, prepojenie s AD |
|  | 10 | Konfigurácia centrálneho manažmentu a príprava správcovského template, ktorý bude implementovaný na všetkých pobočkách. Template musí obsahovať minimálne tieto vlastnosti:   1. IP adresa pre pripojenie pobočkového firewallu do existujúcej manažovacej siete 2. Nastavenie základných sieťových protokolov: DNS, NTP, Syslog, SNMP 3. Pripojenie firewallov do existujúceho Security Fabric riešenia – FortiClient EMS Cloud 4. Pripojenie firewallov do existujúceho logovacieho zariadenia 5. Pripojenie firewallov ku overovacím serverom, ktoré slúžia na overovanie identity prihlasujúceho administrátora (tacacs alebo radius) – verejný obstarávateľ vyšpecifikuje |
|  | 11 | Konfigurácia centrálneho manažmentu a príprava upgrade template, ktorý bude slúžiť na upgrade všetkých pripojených sieťových zariadení na verziu operačného systému podľa požiadavky verejného obstarávateľa. |
|  | 12 | Zaregistrovanie zariadení, licencíí a podpory podľa požiadaviek výrobcu. Príprava evidencie na distribúciu jednotlivých sieťových prvkov pre jednotlivé pobočky |
|  | 13 | Doručenie jednotlivých zariadení na pobočky a ich fyzické pripojenie do siete a manažmentovej siete |
|  | 14 | Konfigurácia centrálneho manažmentu a aplikácia správcovského a upgrade template, podľa požiadaviek vyššie. |
|  | 15 | Dokumentácia aktuálne pripojených portov na jednotlivých pobočkách |
|  | 16 | Konfigurácia zón a jednotlivých L2 vlan – nastavenie základných bezpečnostných prístupových pravidiel na týchto vlan podľa požiadaviek verejného obstarávateľa |
|  | 17 | Nastavenie NAC politík. Tieto politiky umožnia automatické priraďovanie vlan na pripojený prístupový port |
|  | 18 | Import a kontrola ZTNA tagov z existujúceho FortiClient EMS Cloud riešenia |
|  | 19 | Aplikácia NAC politík na jednotlivé prístupové porty |
|  | 20 | Preklopenie nastavení používateľských portov z access switchov HPe do NAC politík na automatické priraďovanie vlan na portoch |
|  | 21 | Prepojenie patch káblov z access switchov HPe do dodávaných access switchov |
|  | 22 | Migrácia existujúcich firewallových pravidiel (ACL) z HPe GW zariadení |
|  | 23 | Konsolidácia firewallových pravidiel (ACL) a doplnenie ZTNA tagov do týchto politík, kvôli implementácií ZTNA – zero trust network access riešenia |
|  | 24 | Konfigurácia smerovania prevádzky s využitím statických ale aj dynamických smerovacích protokolov medzi objektami NBS |
|  | 25 | Vytvorenie projektovej, prevádzkovej a technickej dokumentácie |
|  | 26 | Zaistenie konfigurácie automatického zálohovania systému |
|  | 27 | Nastavenie integrácie so SIEM riešením (LogRhythm), t.j. minimálne posielanie auditných a bezpečnostných udalostí vo formáte a spôsobom, ktorý LogRhythm pre danú technológiu podporuje. |
|  | 28 | Nastavenie mailovej notifikácie, pravidelného reportingu |
|  | 29 | Konfigurácia SNMP (v3) |
|  | 30 | Konfigurácia bezpečnostných nastavení  Uchádzač predloží návrh na hardening a bezpečnostnú konfiguráciu zariadení, (všetkých využívaných funkcií a sieťových protokolov) ktorú po odsúhlasení verejným obstarávateľom nasadí v dodávanom riešení |
|  | 31 | Uchádzač zabezpečí realizáciu prezentáciu pre správcov zadávateľa v priestoroch zadávateľa pre dodané zariadenia a systémy v rozsahu umožňujúcom správcom vykonávať:  • bežnú rutinnú prevádzku a údržbu dodaného systému, vrátane vykonania príslušných konfiguračných zmien,  • diagnostiku a riešenie problémov s funkčnosťou a dostupnosťou HW  • tvorbu reportov. |
|  | 32 | Integrácia do existujúceho managementu verejného obstarávateľa (FortiManager) prevádzkovaného verejným obstarávateľom |
|  | 33 | Nastavenie learning módu a až následne aktivácia blokovacieho módu |
|  | 34 | Konfigurácia firewall pravidiel na základe príslušnosti identít z AD a implementácia ZTNA tagov z Forticlient EMS cloud riešenia |
|  | 35 | Konfigurácia clustrov na dodávaných smerovačoch typ 1. vytvorenie MCLAG – multichassis link aggregation |
|  | 36 | Aktivácia AV engine, a IPS/IDS ochrany |

* 1. Po ukončení inštalačných a konfiguračných prác podľa bodu 2.1 bude vykonané akceptačné testovanie, ktoré vykoná verejný obstarávateľ, v lehote do desiatich pracovných dní po dokončení inštalačných a konfiguračných prác uchádzačom. Akceptačné testy budú ukončené nahlásením výsledku uchádzačovi a odovzdaním zoznamu nájdených vád. Po odstránení vád uchádzačom verejný obstarávateľ akceptačné testy zopakuje, najviac však 1x. V prípade, že budú aj po opakovanom akceptačnom testovaní nájdené vady, bude testovanie vyhodnotené ako neúspešné.
  2. Verejný obstarávateľ prevezme zhotovené dielo po úspešnom ukončení akceptačného testovania formou podpisu záverečného akceptačného protokolu. Uchádzač je na základe podpísaného akceptačného protokolu verejným obstarávateľom oprávnený vystaviť faktúru so splatnosťou 30 dní. V prípade, že akceptačné testovanie nebude úspešné, je verejný obstarávateľ oprávnený odstúpiť okamžite od zmluvy, pričom uchádzačovi nevzniká žiadny nárok na úhradu nákladov za dovtedy poskytnuté služby.

1. Projektové požiadavky

Verejný obstarávateľ požaduje od uchádzača, aby bol projekt riadený na základe metodiky, ktorú určuje pracovný predpis verejného obstarávateľa č. 20/2020 o projektovom riadení (založená na princípoch metodiky PRINCE2) a  na základe projektových požiadaviek, ktoré sú uvedené v týchto súťažných podkladoch – Projektové požiadavky.



1. Servisná podpora a údržba

Verejný obstarávateľ požaduje, aby služba Servisná podpora a údržba bola poskytovaná po dobu 60 mesiacov. Špecifikácia a popis servisnej podpory a údržby je uvedený v odstavcoch 4.1 Podpora a 4.2 Údržba.

* 1. Podpora
     1. Popis služieb Podpora je uvedený v Tabuľke č. 12. Uchádzač sa zaväzuje poskytovať službu Podpora v súlade s Tabuľkou č. 12.
     2. Služba Podpora poskytovaná uchádzačom verejnému obstarávateľovi a zahrňuje aj koordináciu a riadenie poskytovania Servisných služieb poskytovaných verejnému obstarávateľovi podľa servisnej zmluvy.
     3. Uchádzač v rámci služby Podpora bude vykonávať odsúhlasenie zmien a/alebo rozšírení dodaného systému odovzdaných verejnému obstarávateľovi nasledujúcim, alebo iným vzájomne odsúhlaseným postupom.
     4. Uchádzač v rámci služby Podpora bude vykonávať odsúhlasenie zmien a/alebo rozšírení dodaného systému odovzdaných verejnému obstarávateľovi nasledujúcim alebo iným vzájomne odsúhlaseným postupom.

Postup odsúhlasenia zmien poskytnutých Verejný obstarávateľom:

* + - 1. Verejný obstarávateľ zaeviduje prostredníctvom systému Service Desk požiadavku na vykonanie zmien a/alebo rozšírení a popíše požadované zmeny a/alebo rozšírenia dodaného systému.
      2. Uchádzač posúdi a potvrdí správnosť popisu navrhovanej zmeny a/alebo rozšírenia dodaného systému, prípadne ho doplní a dodá postup na vykonanie zmeny a/alebo rozšírenia v dodanom systéme, prípadne požiada verejného obstarávateľa o doplnenie.
      3. Verejný obstarávateľ v zmysle uchádzačom dodaného postupu zrealizuje navrhovanú zmenu a/alebo rozšírenie dodaného systému.
      4. v prípade úspešného vykonania zmeny a/alebo rozšírenia dodaného systému verejný obstarávateľ potvrdí správnosť vykonanej činnosti.

*Tabuľka č. 12 – Popis služby Podpora*

| **ID** | **Činnosti** | **Aktivácia služby** | | | **Úroveň služby** | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Spúšťač** | **Frekvencia** | **Štart** | **Dostupnosť služby** | **Doba odozvy** | **Lehota služby** |
|  | Poskytovanie konzultácií (telefonicky, e-mailom) súvisiacich s problematikou funkcionality, administrácie, prevádzky dodaného systému a jeho častí, pri zmenách konfigurácie dodaného systému | Žiadosť | - | - | v pracovnej dobe v čase od 7.00 h do 18.00 h | operatívne | 2 pracovné dni |
|  | poskytovanie informácie o prípadných predporuchových a poruchových stavoch dodaného systému a bezodkladné informovanie verejného obstarávateľa o závažných bezpečnostných zraniteľnostiach v dodaných komponentoch (s CVSSv3 skóre aspoň 7, alebo ktoré ako závažné označil výrobca), vrátane návrhu plánu na ich odstránenie v infraštruktúre verejného obstarávateľa | zistenia | - | - | v pracovnej dobe v čase od 8.00 h do 17.00 h | operatívne | 2 pracovné dni |
|  | Predkladanie návrhov na zlepšenie výkonnosti dodaného systému | Kalendár | 1 x ročne | VI. | v pracovnej dobe v čase od 8.00 h do 17.00 h | - | 10 pracovných dní |
|  | sledovanie a vyhodnocovanie odporúčaní výrobcu vo vzťahu k zaisteniu spoľahlivej a bezpečnej prevádzky zariadení:   * programového vybavenia všetkých produktov, * softvéru pre správu sieťovej infraštruktúry, * operačného systému po užívaného na zabezpečenie prevádzky softvéru pre správu sieťovej infraštruktúry.   a informovať Verejný obstarávateľa o ich vydaní | Kalendár | 2 x ročne | I, VI. | v pracovnej dobe v čase od 8.00 h do 17.00 h | - | 10 pracovných dní |
|  | * vykonávanie fyzickej inštalácie/reinštalácie zariadení, inštalácie a aktualizácie OS zariadení, resp. OS modulov z ktorých zariadenie pozostáva, * vykonávanie konfigurácie a zmien konfigurácie zariadení podľa požiadaviek verejného obstarávateľa, aktualizácia dokumentácie * vykonávanie inštalácie odporúčaní výrobcu na základe odporúčania uchádzača a po odsúhlasení verejným obstarávateľom | Žiadosť | - | - | v pracovnej dobe v čase od 8.00 h do 17.00 h | operatívne | 5 pracovných dní |
|  | Posudzovanie návrhov Verejný obstarávateľa na zmeny nastavenia a konfigurácie dodaného systému v rozsahu do 1 MD / 1 požiadavka na zmenu | Žiadosť | - | - | v pracovnej dobe v čase od 8.00 h do 17.00 h | 24 h | 5 pracovných dní |
|  | Poskytovanie konzultácií (telefonicky, e-mailom) súvisiacich s možnosťami ďalšieho rozvoja a rozšírenia dodaného systému | Žiadosť | - | - | v pracovnej dobe v čase od 8.00 h do 17.00 h | 24 h | 10 pracovných dní |

* 1. Údržba
     1. Predmetom poskytovania služby "Údržba" je riešenie a odstraňovanie prevádzkových incidentov klasifikovaných v tabuľke č. 13 - Klasifikácia incidentov podľa závažnosti ako „Zásadný incident“ a „Závažný incident“ bez ohľadu na to, či príčinou prevádzkového incidentu sú zmeny a/alebo rozšírenia dodaného systému realizované uchádzačom a/alebo verejným obstarávateľom.

*tabuľka č. 13 – Klasifikácia incidentov podľa závažnosti*

|  |  |
| --- | --- |
| Zásadný incident | Do tejto kategórie spadajú všetky incidenty spojené s používaním a prevádzkou dodávaného systému a oznámené uchádzačovi verejným obstarávateľom, u ktorých sa riešením incidentu zistí, že je spôsobený vážnym nedostatkom dodávaného systému a tento nedostatok **zabraňuje** jeho používaniu v prevádzke nasledovne:   1. neumožňuje používateľom NBS využívať IT služby pri výkone ich pracovných činností, 2. neumožňuje správnu funkčnosť komponentov IT infraštruktúry ako sú napr. servery, 3. znižuje výkon alebo priepustnosť zariadení o vyše 50%   Typicky sa jedná o poruchy zariadení, ktoré nie sú redundantné na úrovni služby, resp. poruchy komponentov, ktoré nie sú redundantné v rámci zariadenia. |
| Závažný incident | Do tejto kategórie spadajú všetky incidenty spojené s používaním a prevádzkou dodávaného systému a oznámené uchádzačovi verejným obstarávateľom, u ktorých sa riešením incidentu zistí, že je spôsobený nedostatkom dodávaného systému a tento nedostatok **nespôsobí výpadok** funkčnosti dodaného systému alebo ktorejkoľvek jeho časti a tento výpadoknenaruší poskytovanie sieťových služieb v rámci NBS |

* + 1. Verejný obstarávateľ požaduje, aby klasifikácia incidentov podľa závažnosti, ktorá je uvedená v tabuľke č. 13 platila pre servis dodávaného systému počas záručnej doby a aj po záručnej dobe. Klasifikáciu incidentov stanovuje poverený zamestnanec verejného obstarávateľa podľa závažnosti.
    2. Verejný obstarávateľ pripúšťa, že uchádzač môže na základe vykonanej analýzy incidentu požiadať verejného obstarávateľa o zmenu klasifikácie incidentu. O zmene klasifikácie incidentu rozhoduje poverený zamestnanec verejného obstarávateľa na základe analýzy incidentu predloženej uchádzačom.
    3. Verejný obstarávateľ požaduje, aby sa uchádzač zaviazal poskytovať službu Údržba v súlade s tabuľkou č. 14.

*Tabuľka č. 14 – Popis služby Údržba*

| **ID** | **Činnosti** | **Aktivácia služby** | | | **Úroveň služby** | |
| --- | --- | --- | --- | --- | --- | --- |
| **Spúšťač** | **Frekvencia** | **Štart** | **Dostupnosť služby** | **Lehota služby** |
|  | Poskytovanie informácií (telefonicky) súvisiacich s chybovými hláseniami dodaného systému | Nahlásenie incidentu | - | - | v pracovnej dobe | do 4 h |
|  | Riešenie a odstránenie incidentov klasifikovaných. ako: **„Zásadný incident**“ so zaručeným časom odstránenia incidentu v mieste inštalácie od písomného alebo vzájomne odsúhlaseného spôsobu nahlásenia tohto incidentu zo strany verejného obstarávateľa alebo od jeho detegovania uchádzačom | Nahlásenie / diagnostikovanie incidentu | - | - | v pracovnej dobe | do 8 h |
|  | Riešenie a odstránenie incidentov klasifikovaných ako: **„Závažný incident“** so zaručeným časom odstránenia incidentu v mieste inštalácie od písomného alebo vzájomne odsúhlaseného spôsobu nahlásenia tohto incidentu zo strany verejného obstarávateľa alebo od jeho detegovania uchádzačom | Nahlásenie / diagnostikovanie incidentu | - | - | v pracovnej dobe | najneskôr do 17.00 h nasledujúceho pracovného dňa |
|  | Súčinnosť pri verejným obstarávateľom odstraňovaných poruchách externých systémov súvisiacich s dodaným systémom. | žiadosť | - | - | v pracovnej dobe | Do 4 h |
|  | Súčinnosť pri nasadení verejným obstarávateľom odsúhlasených opravných balíčkov (patch) do SW tretích strán. | Kalendár | dohodou | - | - | dohodou |
|  | Aktualizácia dokumentácie k dodanému systému v súvislosti s opravou incidentov dodaného systému | Kalendár | priebežne | - | - | 5 pracovných dní |

* + 1. Pri poskytovaní služby Údržba je Lehota služby stanovená vo vyššie uvedenej tabuľke č. 14 bodu 4.2.4 záväzná aj v prípade, ak by pri jednotlivých činnostiach služby Údržba požadovaných verejným obstarávateľom počas Dostupnosti služby malo jej dodržanie prekročiť hornú hranicu stanovenej pracovnej doby.
    2. Uchádzač sa zaväzuje v rámci služby Údržba, že pri výmene komponentu IT infraštruktúry a/alebo časti komponentu IT infraštruktúry dodá komponent IT infraštruktúry a/alebo časť komponentu IT infraštruktúry rovnakých alebo vyšších parametrov.
    3. Uchádzač sa zaväzuje v rámci služby Údržba používať nasledovný postup evidovania prevádzkových incidentov v systéme pre evidenciu incidentov verejného obstarávateľa:
    - Verejný obstarávateľ alebo Uchádzač zaeviduje prevádzkový incident dodaného systému,
    - Uchádzač analyzuje prevádzkový incident a v rámci analýzy uvedie príčinu incidentu,
    - Uchádzač vyrieši prevádzkový incident a v rámci riešenia uvedie:
      * spôsob vyriešenia prevádzkového incidentu,
      * dopad na produktovú dokumentáciu prípadne aj aktualizovanú príslušnú časť produktovej dokumentácie,
      * postup na inštalovanie riešenia prevádzkového incidentu,
      * či riešenie má alebo nemá vplyv na riešenie iných incidentov,
    - Uchádzač dodá riešenie prevádzkového incidentu dohodnutým spôsobom, aby pri implementovaní (nasadení) riešenia prevádzkového incidentu nedochádzalo k vzniku nových prevádzkových incidentov,
    - Verejný obstarávateľ vráti incident na doriešenie uchádzačovi v prípade, že prevádzkový incident nie je odstránený,
    - Verejný obstarávateľ uzavrie riešenie prevádzkového incidentu a vypracuje protokol o testovaní, alebo uvedie informáciu o výsledkoch testovania do systému pre evidenciu incidentov Verejný obstarávateľa v prípade odstránenia prevádzkového incidentu,
    - Verejný obstarávateľ môže požiadať uchádzača o účasť pri overení riešenia prevádzkového incidentu a Uchádzač vyvinie primerané úsilie, aby sa mohol overenia zúčastniť,
    1. Uchádzač môže na odstránenie incidentov uvedených v tabuľke č. 13 „Klasifikácia incidentov podľa závažnosti“ tejto prílohy s Lehotami služieb uvedenými v tabuľke č. 14 tejto prílohy použiť náhradné riešenie.
    2. Ak sa verejný obstarávateľ a uchádzač nedohodnú inak, náhradné riešenie, ktoré eliminovalo vážne chyby alebo nedostatky spôsobujúce zásadný incident systému bude nahradené odstránením vážnej chyby alebo nedostatku v lehote do 4 pracovných dní a náhradné riešenie, ktoré eliminovalo chyby a/ alebo nedostatky spôsobujúce závažný incident systému bude nahradené odstránením chyby alebo nedostatku v lehote do 7 pracovných dní po ich nahlásení.

1. Konzultačné a dodatočné implementačné služby
   1. Konzultačné a dodatočné implementačné služby budú poskytované uchádzačom počas trvania servisnej zmluvy v maximálnom rozsahu 60 MD.
   2. Uchádzač sa zaväzuje, že bude poskytovať konzultačné a implementačné služby na zariadenia certifikovaným zamestnancom na príslušnú technológiu.
   3. Predmetom poskytovania služby Implementácia sa pre účely tohto obstarávania rozumie služba umožňujúca
      * analýzu požiadaviek verejného obstarávateľa a návrh riešenia a
      * úpravu dodaného systému podľa požiadaviek verejného obstarávateľa s cieľom zabezpečiť zlepšenie existujúcej a/alebo dodanie novej funkčnosti do dodaného systému.
   4. Uchádzač sa zaväzuje poskytnúť verejnému obstarávateľovi službu Implementácia, ak o vykonanie tejto služby verejný obstarávateľ požiada formou písomnej záväznej objednávky vystavenej a doručenej uchádzačovi a v množstve v akom o to verejný obstarávateľ touto záväznou písomnou objednávkou požiada.

Uchádzač sa zaväzuje poskytovať službu Implementácia v súlade s tabuľkou č. 15.

*Tabuľka č. 15 - Popis služby Implementácia*

| **ID** | **Služba / Činnosti** | **Aktivácia služby** | | | **Úroveň služby** | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Spúšťač** | **Frekvencia** | **Štart** | **Dostupnosť služby** | **Doba odozvy** | **Lehota služby** |
| 1. | Vykonať predbežnú analýzu a vypracovať písomnú ponuku na analýzu požiadavky a na návrh riešenia | Žiadosť | - | - | v pracovnej dobe  čase od 8.00 h do 17.00 h | - | do 5 pracovných dní |
| 2. | Vykonať analýzu požiadavky a vypracovať návrh riešenia | Žiadosť / Objednávka | - | - | v pracovnej dobe  čase od 8.00 h do 17.00 h | - | podľa objednávky |
| 3. | Realizácia požiadavky, aktualizácia sprievodnej dokumentácie dodaného systému | Objednávka | - | - | v pracovnej dobe  čase od 8.00 h do 17.00 h | - | podľa objednávky |

* 1. Uchádzač sa zaväzuje poskytovať službu Implementácie nasledujúcim spôsobom:
     + verejný obstarávateľ zašle uchádzačovi požiadavku na predbežnú analýzu,
     + uchádzač vypracuje ponuku na analýzu predmetu požiadavky a na návrh riešenia,
     + verejný obstarávateľ vyhodnotí ponuku na analýzu predmetu požiadavky a na návrh riešenia a v prípade jej akceptovania zašle uchádzačovi záväznú objednávku na vypracovanie analýzy požiadavky a návrhu riešenia,
     + uchádzač vykoná analýzu predmetu požiadavky verejného obstarávateľa a vypracuje návrh riešenia a
     + verejný obstarávateľ vyhodnotí návrh riešenia a v prípade jeho akceptovania a prijatia rozhodnutia o realizácii požiadavky zašle uchádzačovi objednávku na realizáciu riešenia,
     + v prípade rozsiahlej požiadavky verejný obstarávateľ môže požiadať uchádzača najprv o vypracovanie ponuky na analýzu predmetu požiadavky a jej realizáciu a následne o vypracovanie ponuky na návrh riešenia a samotnú realizáciu riešenia.
  2. Požiadavka týkajúca sa poskytnutia služby Implementácie bude v písomnej forme odovzdaná uchádzačovi na predbežnú analýzu. Táto požiadavka musí obsahovať:
     + názov požiadavky a poradové číslo požiadavky,
     + popis a dôvod požadovaných úprav,
     + očakávané dopady týchto úprav – napr. nová funkčnosť a pod. a
     + podpis oprávnenej osoby na strane verejného obstarávateľa.
  3. Verejný obstarávateľ požaduje, aby uchádzač na základe požiadavky verejného obstarávateľa na predbežnú analýzu najneskôr do 5-tich pracovných dní od obdržania požiadavky vypracoval písomnú ponuku na analýzu požiadavky a na návrh riešenia. Táto písomná ponuka musí obsahovať:
     + odkaz na pôvodnú požiadavku,
     + záväznú cenu za analýzu a návrh riešenia,
     + dobu realizácie a termín ukončenia,
     + predbežný návrh harmonogramu analýzy spolu s popisom činností, ktoré plánuje vykonať počas analýzy a návrhu riešenia a
     + podpis(y) zodpovedného(ých) zástupcu(ov) uchádzača.
  4. Verejný obstarávateľ na základe vyhodnotenia ponuky rozhodne o prijatí alebo odmietnutí tejto ponuky. V prípade odmietnutia ponuky môže navrhnúť uchádzačovi, aby prehodnotil ponuku a predložil novú ponuku na analýzu požiadavky a na návrh riešenia. Po schválení ponuky verejný obstarávateľ vystaví objednávku na analýzu požiadavky a návrh riešenia, pričom v objednávke zohľadní uchádzačom navrhovanú dobu realizácie. Analýzu požiadavky a návrh riešenia realizuje uchádzač až po obdržaní objednávky na analýzu požiadavky a návrh riešenia, a to najneskôr do termínu určeného v objednávke.
  5. Verejný obstarávateľ požaduje, aby uchádzač na základe objednávky analyzoval požiadavku verejného obstarávateľa a písomne navrhol riešenie spolu s návrhom harmonogramu implementácie a pevnej ceny. Návrh riešenia musí obsahovať:
     + odkaz na pôvodnú požiadavku,
     + detailný popis riešenia (doplnkom sú i odkazy do pôvodnej dokumentácie) a jeho dopad na dodaný systém,
     + záväznú cenu za realizáciu navrhovaného riešenia s rozpisom doby realizácie,
     + predbežný návrh harmonogramu implementácie riešenia s dobou realizáciu navrhovaného riešenia a termínom ukončenia,
     + podpis(y) zodpovedného(ých) zástupcu(ov) uchádzača.
  6. Verejný obstarávateľ na základe vyhodnotenia analýzy a návrhu riešenia rozhodne, či analýzu a návrh riešenia akceptuje a podpíše preberací protokol „Protokol o prijatí analýzy a návrhu riešenia požiadavky v rámci dodaného systému“, pričom dátumom prevzatia je dátum uvedený v protokole o prevzatí. Protokol o prijatí analýzy a návrhu riešenia je vyhotovený v dvoch rovnopisoch, verejný obstarávateľ aj uchádzač obdržia po jednom vyhotovení protokolu o prevzatí.

V prípade, že bude mať verejný obstarávateľ výhrady k vyhodnoteniu analýzy a návrhu riešenia je verejný obstarávateľ oprávnený navrhnúť uchádzačovi, aby prehodnotil predovšetkým navrhovaný spôsob, čas a harmonogram implementácie riešenia a predložil novú analýzu a návrh riešenia.

Ak verejný obstarávateľ rozhodne, že sa požiadavka bude realizovať v súlade s analýzou a návrhom riešenia, zašle uchádzačovi objednávku na realizáciu požiadavky, pričom v objednávke zohľadní uchádzačom navrhovanú dobu realizácie riešenia. K samotnej realizácii riešenia pristúpi uchádzač až po obdržaní objednávky na realizáciu riešenia v termíne stanovenom v objednávke.

* 1. V prípade požiadavky, kde na základe dohody verejného obstarávateľa a uchádzača pre stanovenie spôsobu realizácie požiadavky verejného obstarávateľa, harmonogramu realizácie požiadavky verejného obstarávateľa a pevnej ceny za realizáciu požiadavky verejného obstarávateľa nie je potrebná samostatná analýza požiadavky a návrh riešenia, môže verejný obstarávateľ zaslať objednávku na realizáciu požiadavky bez toho, aby bol dodržaný postup poskytovania služby implementácie popísaný v bode 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, t. j. môže požiadať uchádzača na vytvorenie analýzy a realizáciu riešenia.
  2. Verejný obstarávateľ požaduje, aby bol dodržaný nasledovný postup pri prevzatí upraveného dodaného systému alebo jeho časti:
     + Uchádzač dodá úpravu dodaného systému alebo jeho časti,
     + Uchádzač dodá návrh postupov pre overenie funkčnosti úpravy dodaného systému v termíne, ktorý bude uvedený v návrhu harmonogramu implementácie, avšak najneskôr k termínu dodania riešenia. Verejný obstarávateľ v prípade potreby je oprávnený požiadať uchádzača o zmenu alebo doplnenie uchádzačom predložených návrhov postupov, ktoré Uchádzač po prípadnej konzultácií s Verejný obstarávateľom zapracuje,
     + Uchádzač dodá na jednom médiu oddelene aktualizáciu tej časti inštalačných a používateľských príručiek a technickej dokumentácie dodaného systému, ktorá bola službou dotknutá, a taktiež úplné aktualizované inštalačné a používateľské príručky a technickú dokumentáciu dodaného systému doplnenú o tieto zmeny najneskôr 5 pracovných dní pred začiatkom overenia funkčnosti, pokiaľ nebude vzájomne dohodnuté inak,
     + v prípade, že úprava dodaného systému sa týka IT zariadenia alebo jeho časti Uchádzač dodá úpravu dodaného systému najneskôr v deň overovania jeho funkčnosti ,
     + Verejný obstarávateľ overí funkčnosť upraveného dodaného systému alebo jeho časti v podmienkach verejného obstarávateľa a za účasti uchádzača,
     + Verejný obstarávateľ vyhodnotí úspešnosť overenia na základe splnenia verejný obstarávateľom vypracovaných a vzájomne schválených kritérií, ktoré budú vztiahnuté na počet a závažnosť incidentov,
     + Verejný obstarávateľ potvrdí po úspešnom ukončení overenia prevzatie úpravy dodaného systému alebo jeho časti podpisom preberacieho protokolu o plnení služby Implementácia dodaného systému, ktorého súčasťou bude akceptačný protokol upraveného dodaného systému, alebo jeho časti - „Protokol o akceptačnom testovaní úpravy dodaného systému a o výsledkoch akceptačných testov“, pričom dátumom prevzatia je dátum uvedený v preberacom protokole. Preberací protokol úpravy dodaného systému alebo jeho časti je vyhotovený v piatich rovnopisoch. Verejný obstarávateľ obdrží štyri a uchádzač jedno vyhotovenie preberacieho protokolu,
     + súčasťou dodávky úpravy dodaného systému budú aj postupy, na základe ktorých bude môcť Verejný obstarávateľ vykonávať zmeny a/alebo rozšírenia dodaného systému bez predchádzajúceho súhlasu uchádzača.
  3. Platba za analýzu požiadavky a návrh riešenia bude realizovaná na základe verejným obstarávateľom podpísaného preberacieho protokolu plnenia služby a k nej uchádzačom vystavenej faktúry podľa objednávky na analýzu požiadavky a návrh riešenia.

Platba za realizáciu riešenia bude uskutočnená na základe verejným obstarávateľom podpísaného preberacieho protokolu plnenia služby a k nej uchádzačom vystavenej faktúry podľa objednávky na realizáciu riešenia.