

## ŠPECIFIKÁCIA PREDMETU KÚPY

### **Opis predmetu zákazky k výzve v rámci DNS na predmet zákazky: Nákup IKT (DNS)\_Obstaranie bezpečnostných komponentov NCZI**

Predmetom zákazky je dodávka infraštruktúry, ktorá pozostáva zo:

- OOB Firewall,
- Backup Firewall,
- Centrálny systém SDDC firewallu,
- Emailová brána,
- PAM Server
- Centrálna autentizácia, autorizácia a účtovanie (AAA) + systém viacfaktorovej autentizácie (MFA),

Zahrnuté sú aj služby spojené s dopravou, montážou, inštaláciou a nastavením zariadení, ako aj prípadnou inicializáciou a konfiguráciou softvéru, aby bolo zabezpečené, že dodaná infraštruktúra je plne funkčná a prevádzkyschopná.

#### **Slovný opis požiadaviek:**

Predmetom zákazky je dodávka tovarov a softvérových licencií, vrátane inštalačnej služby, ktorá zahŕňa nasledovné komponenty:

1. **Systém pre zabezpečenie služby OOB Firewall:** Dodávka, doprava, montáž a inštalácia systému, ktorý poskytuje vlastnosti next-gen firewallu pre potreby vybudovania Out-of-Band (OOB) manažmentovej siete softvérovo definovaného dátového centra (SDDC). Služba zahŕňa inštaláciu, konfiguráciu a inicializáciu systému.
2. **Systém pre zabezpečenie zálohovacích služieb SDDC prostredia formou Backup Firewall:** Dodávka, doprava, montáž a inštalácia záložného firewallu, poskytujúceho vlastnosti next-gen firewallu pre vytvorenie zabezpečeného VPN tunela medzi NCZI a SDDC prostredím. Súčasťou služby je inštalácia, konfigurácia a inicializácia softvéru.
3. **Centrálny systém pre zabezpečenie služby interného SDDC firewallu:** Dodávka, doprava, montáž a inštalácia centrálného firewallového systému, ktorý poskytuje next-gen firewallové vlastnosti pre potreby softvérovo definovanej sieťovej infraštruktúry (SDN). Služba zahŕňa inštaláciu, konfiguráciu a inicializáciu softvéru.
4. **Emailová brána:** Dodávka, doprava, montáž a inštalácia softvérového riešenia, ktoré zabezpečuje komplexnú ochranu e-mailovej komunikácie organizácie pred rôznymi bezpečnostnými hrozbami, vrátane škodlivých útokov, phishingu, spamu a pokročilých hrozieb. Súčasťou služby je inštalácia, konfigurácia a inicializácia softvéru.
5. **Privileged Access Management (PAM) server:** Dodávka, doprava, montáž a inštalácia softvérového riešenia pre centralizovanú správu a ochranu privilegovaných účtov a prístupov v rámci organizácie. Inštalačná služba zahŕňa inštaláciu, konfiguráciu a inicializáciu softvéru.
6. **Centrálna autentizácia, autorizácia a účtovanie (AAA) + systém viacfaktorovej autentizácie (MFA):** Dodávka, doprava, montáž a inštalácia systému na centralizované riadenie prístupu používateľov k sieťovým zdrojom a službám, doplneného o viacfaktorovú autentizáciu (MFA). Inštalačná služba zahŕňa inštaláciu, konfiguráciu a inicializáciu softvéru.

Všetky komponenty uvedené v konfigurácii ponúkaného predmetu zákazky musia byť certifikované výrobcom daného predmetu zákazky (originálne príslušenstvo). Každý funkčný celok má detailne špecifikované požadované parametre jednotlivých zariadení.

## 1. OOB Firewall

Tabuľka č. 1

| Parameter:  | Minimálne požadované parametre:   | Hodnota:   | Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru   |
|---|---|--|--|
| <p><b>Systém pre zabezpečenie služby OOB FW, poskytujúceho vlastnosti next-gen firewallu pre potreby vybudovania OOB manažmentovej siete SDDC.</b><br/> <b>Je nutné uviesť detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (Part Number, Product Code)</b></p> |   |  | <p>OOB Firewall od výrobcu Fortinet, Inc. s Product Code: FG-121G, ktorý bude obsahovať uvedenú detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (product code):</p> <p>2x FG-121G<br/>         6x FC-10-F121G-950-02-12<br/>         2x FG-VDOM-5-UG<br/> <a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-120g-series.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-120g-series.pdf</a><br/> <a href="https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/954635/getting-started">https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/954635/getting-started</a><br/> <a href="https://docs.fortinet.com/product/fortigate/7.6">https://docs.fortinet.com/product/fortigate/7.6</a></p> <p>2x FC1-10-FMGVS-258-01-36<br/>         15x FC-10-FMGVS-230-01-12<br/> <a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf</a><br/> <a href="https://docs.fortinet.com/product/fortimanager/7.4">https://docs.fortinet.com/product/fortimanager/7.4</a></p> |
| <b>Počet:</b>   | 2 ks<br>Dodané riešenie musí byť vo forme fyzických zariadení s výnimkou manažmentu riešenia, ktoré musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu. |  | v počte 2ks bude vo forme fyzických zariadení s výnimkou manažmentu riešenia, ktoré bude vo forme virtuálneho zariadenia pre virtualizačnú platformu.  |
|   | Priepustnosť Firewallu podľa RFC 3511, 2544, 2647, 1242   | Min. 35 Gb/s   | Firewall FortiGate 121G podľa RFC 3511, 2544, 2647, 1242 dosahuje priepustnosť až 39 Gb/s  |
|   | Priepustnosť IPS podľa RFC 3511, 2544, 2647, 1242   | Min. 5 Gb/s  | Priepustnosť IPS podľa RFC 3511, 2544, 2647, 1242 je 5,3 Gb/s.   |
|   | Priepustnosť so zapnutou ochranou pred hrozbami (threat protection – antimalware, IPS, application control)   | Min. 2,5 Gb/s  | Priepustnosť so zapnutou ochranou pred hrozbami (threat protection – antimalware, IPS, application control) je 2,8 Gb/s.   |
|   | Priepustnosť IPsec VPN (512 bytes)  | Min. 35 Gb/s   | Priepustnosť IPsec VPN (512 bytes) je 35 Gb/s.   |
|   | Priepustnosť SSL VPN  | Min. 1,5 Gb/s  | Priepustnosť SSL VPN je 1,5 Gb/s.  |
|   | Latencia (64 byte, UDP)   | Menej ako 3,2 mikrosekúnd (64 byte UDP)  | Latencia (64 byte, UDP) je 3,17 mikrosekúnd  |
|   | Počet nových spojení za sekundu (CPS)   | Min. 140 000   | Podporuje 140 000 nových spojení za sekundu.   |
|   | Počet súčasných spojení   | Min. 3 000 000   | Podporuje 3 000 000 súčasných spojení.   |
|   | Počet fyzických sieťových rozhraní  | Min. 16x GE RJ45<br>Min. 2x HA RJ45 port<br>Min. 4x 10 GE SFP+<br>Min. 8x GE SFP | má 16x GE RJ45 portov.<br>má 2x HA RJ45 port.<br>má 4x 10 GE SFP+ sloty<br>má 8x GE SFP sloty.   |
|   | Podpora virtuálnych domén / kontextov   | Min. 10  | Podporuje 10 virtuálnych domén.  |

|                                  |   |             |  |
|----------------------------------|---|-------------|--|
|                                  | Podpora pre lokálne úložisko  | min. 480 GB | Disponuje 480 GB interným SSD úložiskom.   |
| <b>Požadovaná funkcionálnosť</b> | Podpora vysokej dostupnosti v konfigurácii Active-Passive, alebo Active-Active alebo Clustering   |             | FortiGate 121G podporuje vysokú dostupnosť (HA) v režimoch Active-Passive aj Active-Active, čo umožňuje nasadenie v klastroch pre zvýšenú spoľahlivosť a výkon.  |
|                                  | Podpora synchronizácie TCP, UDP spojení a sieťových prekladov   |             | FortiGate 121G podporuje synchronizáciu TCP, UDP spojení a sieťových prekladov   |
|                                  | Podpora Site to Site IPSEC tunelov.   |             | FortiGate 121G podporuje vytváranie IPsec VPN tunelov pre bezpečnú komunikáciu medzi rôznymi lokalitami.   |
|                                  | Podpora 802.1Q VLAN, podpora 802.3ad pasívnej a aktívnej agregácie liniek.  |             | FortiGate 121G podporuje štandard 802.1Q pre VLAN trunking a tiež 802.3ad pre agregáciu liniek (LACP), čo umožňuje zvyšovať priepustnosť a redundanciu sieťových pripojení.  |
|                                  | Firewall, IPS, Aplikačná kontrola, Malware a Botnet ochrana.  |             | S licenciou <b>FC-10-F121G-950-02-12</b> zariadenie FortiGate 121G poskytuje funkcie firewallu, systému prevencie prienikov (IPS), aplikačnej kontroly, ochrany pred malvérom a botnetmi.  |
|                                  | Možnosť integrácie s externou Sandbox službou (cloud alebo on-premises).  |             | FortiGate 121G umožňuje integráciu s FortiSandbox pre pokročilú analýzu hrozieb, dostupnú ako cloudová služba alebo on-premises riešenie.  |
|                                  | Musí realizovať filtrovanie tokov na základe doménovej / IP reputácie.  |             | FortiGate 121G využíva FortiGuard služby na hodnotenie reputácie domén a IP adries, čo umožňuje filtrovanie na základe týchto kritérií.  |
|                                  | Musí podporovať filtrovanie web tokov na základe DNS requestov, url filtrovanie a blokovanie na známe botnet a C&C adresy   |             | FortiGate 121G podporuje DNS filtrovanie, URL filtrovanie a ochranu proti botnetom prostredníctvom FortiGuard služieb, čo umožňuje blokovanie škodlivých adries a komunikácie s riadiacimi servermi.   |
|                                  | Musí podporovať inšpekciu certifikátov počas SSL handshaku, bez potreby dešifrovania.   |             | FortiGate 121G podporuje inšpekciu SSL/TLS certifikátov počas handshaku, čo umožňuje overenie platnosti certifikátov bez úplného dešifrovania komunikácie.   |
|                                  | Musí umožňovať filtrovanie na základe geografickej lokality.  |             | FortiGate 121G umožňuje filtrovanie a kontrolu prístupu na základe geografickej polohy IP adries, čo umožňuje obmedziť alebo povoliť prístup z konkrétnych regiónov.   |
|                                  | Okamžite použiteľné preddefinované IPS politiky.  |             | FortiGate 121G obsahuje preddefinované politiky pre systém prevencie prienikov (IPS), ktoré sú okamžite použiteľné na ochranu siete pred známymi hrozbami.   |
|                                  | Možnosť nastavenia monitorovacieho alebo blokovacieho režimu IPS globálne, na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry.   |             | Administrátori môžu konfigurovať IPS v monitorovacom (detekčnom) alebo blokovacom (preventívnom) režime na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry.   |
|                                  | Automatické vypnutie IPS ochrany firewallu v prípade preťaženia   |             | FortiGate 121G je navrhnutý tak, aby v prípade preťaženia systému mohli upraviť alebo dočasne deaktivovať niektoré bezpečnostné funkcie, ako je IPS, aby sa zachovala základná funkčnosť siete.  |
|                                  | Podpora pre grafické rozhranie cez HTML 5   |             | Webové administratívne rozhranie FortiGate 121G je založené na HTML5, čo umožňuje prístup a správu zariadenia prostredníctvom moderných webových prehliadačov bez potreby dodatočných pluginov.  |
| <b>Centrálna správa</b>          | <ul style="list-style-type: none"> <li>Centrálny manažment musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu (minimálne podpora VMware ESXi).</li> <li>Musí podporovať správu min. 20 zariadení s možnosťou rozširovania pomocou licencie.</li> <li>Musí podporovať externé identity databázy vrátane LDAP databáz.</li> <li>Musí obsahovať intuitívne grafické rozhranie pre IPv4 klientov.</li> <li>Musí mať integrované monitorovacie, reportovacie aj diagnostické schopnosti pre maximálnu kontrolu a viditeľnosť.</li> </ul> |             | <ul style="list-style-type: none"> <li>Centrálny manažment je dostupný ako virtuálne zariadenie kompatibilné s rôznymi virtualizačnými platformami vrátane VMware ESXi.</li> <li>umožňuje správu min. 20 zariadení, pričom kapacitu je možné rozširovať prostredníctvom licencií podľa potrieb organizácie.</li> <li>podporuje integráciu s externými identitnými službami, vrátane LDAP, čo umožňuje centralizovanú správu užívateľov a autentifikáciu.</li> <li>poskytuje užívateľsky prívetivé grafické rozhranie pre IPv4 klientov založené na HTML5, ktoré je prístupné cez moderné webové</li> </ul> |

|                         |   |   |
|-------------------------|---|---|
|                         | <ul style="list-style-type: none"> <li>Podpora multitenantnosti – oddelené domény pre tenantov a role-based administratorké účty.</li> <li>Podpora automatizovaného REST API, skriptov.</li> <li>Podpora vysokej dostupnosti</li> <li>Podpora pre zamknutie politik pre lepsiu kontrolu nad zmenami v multi admin prostredí.</li> <li>Podpora pre automatické zálohovanie konfigurácií a sledovanie zmien pre audit.</li> <li>Podpora pre centrálnu konfiguráciu pomocou šablátov.</li> <li>Podpora centrálnej distribúcie signatúr.</li> <li>Podpora viacerých správco v rôznych úrovni prístupových oprávnení.</li> <li>Podpora odosielania logov na SYSLOG server.</li> <li>Podpora viacerých administratívnych domén / tenantov</li> <li>integrácia do existujúceho Centrálného bezpečnostného, logovacieho a vyhodnocovacieho nástroja, zloženého z technológií: <ul style="list-style-type: none"> <li>IBM QRadar 7.5</li> <li>The Hive Project 4</li> <li>MISP</li> <li>Greycortex Mendel</li> </ul> </li> </ul> | <p>prehliadače.</p> <ul style="list-style-type: none"> <li>obsahuje nástroje na monitorovanie siete, generovanie reportov a diagnostiku, čo poskytuje komplexný prehľad o stave siete a bezpečnostných udalostiach.</li> <li>Prostredníctvom administratívnych domén (ADOM) umožňuje oddelenú správu pre rôznych tenantov a podporuje role-based prístup pre administrátorov.</li> <li>podporuje REST API a skriptovanie, čo umožňuje automatizáciu úloh a integráciu s inými systémami.</li> <li>podporuje konfigurácie vysokej dostupnosti (HA) s automatickým prepnutím v prípade zlyhania, čím zabezpečuje nepretržitú prevádzku.</li> <li>Funkcia uzamknutia politik umožňuje administrátorom kontrolovať a sledovať zmeny v prostredí s viacerými administrátormi, čím sa predchádza neúmyselným úpravám.</li> <li>automaticky zálohuje konfigurácie zariadení a poskytuje revíziu históriu zmien pre účely auditu a obnovy.</li> <li>Pomocou konfiguračných šablón umožňuje efektívne nasadzovať a spravovať nastavenia na viacerých zariadeniach súčasne.</li> <li>umožňuje centralizovanú distribúciu bezpečnostných signatúr a aktualizácií na spravované zariadenia, čím zabezpečuje jednotnú úroveň ochrany.</li> <li>Systém role-based prístupu umožňuje definovať rôzne úrovne oprávnení pre správco podľa ich úloh a zodpovedností.</li> <li>podporuje export logov na externé SYSLOG servery pre centralizované ukladanie a analýzu.</li> <li>Administratívne domény (ADOM) umožňujú segmentáciu správy pre rôznych tenantov alebo oddelenia v rámci jednej inštalácie</li> <li>podporuje integráciu s externými bezpečnostnými a logovacími nástrojmi prostredníctvom štandardizovaných protokolov a API, čo umožňuje jeho začlenenie do existujúcich bezpečnostných riešení zloženého z technológií: <ul style="list-style-type: none"> <li>IBM QRadar 7.5</li> <li>The Hive Project 4</li> <li>MISP</li> <li>Greycortex Mendel.</li> </ul> </li> </ul> |
| <b>Napájacie zdroje</b> | <ul style="list-style-type: none"> <li>redundantné (redundancia 1+1)</li> <li>maximálny výkon jedného zdroja 50W pri 230V</li> <li>Vstup: 100-240VAC, 60-50Hz</li> </ul>  | <ul style="list-style-type: none"> <li>FortiGate 121G je vybavený dvoma internými napájacími zdrojmi, ktoré poskytujú redundanciu pre zvýšenú spoľahlivosť systému.</li> <li>Maximálna spotreba energie jedného zdroja je 47 W</li> <li>FortiGate 121G podporuje vstupné napätie v rozsahu 100-240 V AC pri frekvencii 50-60 Hz, čo zodpovedá bežným napájacím štandardom.</li> </ul>   |
| <b>Záruka</b>           | <ul style="list-style-type: none"> <li>záručná doba min. 3 roky</li> </ul>  | zariadenie Fortinet FortiGate 121G spĺňa požiadavky na záručnú dobu min. 3 roky   |
|                         | <ul style="list-style-type: none"> <li>spôsob servisu v mieste prevádzky, nonstop (8x5xNBD)</li> </ul>  | zariadenie Fortinet FortiGate 121G spĺňa požiadavky na spôsob servisu v mieste prevádzky v režime nonstop (8x5xNBD)   |
| <b>Inštalácia</b>       | <ul style="list-style-type: none"> <li>súčasťou ponuky musí byť inštalačná služba obsahujúca dopravu, montáž, inštalácia a nastavenie dodaných zariadení prípadne softvérov, odskúšanie funkčnosti a</li> </ul>   | <ul style="list-style-type: none"> <li>Súčasťou ponuky je komplexná inštalačná služba, ktorá zahŕňa zabezpečenie dopravy, fyzickú montáž, odbornú inštaláciu a konfiguráciu dodaných zariadení a softvéru. Táto služba zahŕňa aj testovanie funkčnosti a overenie prevádzkovej spoľahlivosti,</li> </ul>  |

|                         |  |   |
|-------------------------|--|---|
|                         | <p>prevádzkyschopnosti, uvedenie do prevádzky, zaškolenie kupujúcim určených osôb, vrátane inštalácie všetkých súčastí operačných prostredí.</p> <ul style="list-style-type: none"> <li>• inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného riešenia pre OOB firewall</li> <li>• uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané riešenie pre OOB firewall. (Poznámka: predmetný certifikát tvorí prílohu č. 4 ku kúpnej zmluve na predmet zákazky, uchádzač tento dokument nemusí predkladať vo svojej ponuke, postačuje, ak ho predloží úspešný uchádzač najneskôr pri podpise zmluvy).</li> </ul>   | <p>uvedenie zariadení do plnej prevádzky a poskytnutie školenia pre určené osoby kupujúceho, vrátane nasadenia všetkých potrebných súčastí operačných systémov.</p> <ul style="list-style-type: none"> <li>• Inštalačné práce budú realizované kvalifikovaným odborníkom s platným certifikátom, ktorý ho oprávňuje vykonávať montáž, konfiguráciu a správu dodávaného riešenia určeného pre OOB firewall.</li> <li>• Ako uchádzač doložíme platný certifikát vydaný priamo výrobcom, producentom alebo autorizovanou osobou, ktorá má oprávnenie na vydávanie takýchto certifikátov pre riešenie súvisiace s OOB firewallom.</li> </ul>  |
| <b>Servisná podpora</b> | <p>3 roky od zakúpenia s nasledujúcimi parametrami:</p> <ul style="list-style-type: none"> <li>• výmena zariadenia v prípade poruchy (RMA) v režime nasledujúci pracovný deň v mieste prevádzky,</li> <li>• včasné poskytovanie bezpečnostných záplat a hotfixov pre produkty v riešení,</li> <li>• poskytovanie softvérových aktualizácií pre produkty v riešení,</li> <li>• centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami:</li> <li>• riešenie servisných prípadov na úrovni riešenia, nie len na úrovni podpory jednotlivých produktov,</li> <li>• podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora,</li> <li>• požaduje sa podpora od výrobcu s previazanosťou na produkty výrobcov tretích strán. Výrobca poskytne podporu pri riešení prípadu s iným výrobcom v rozsahu platnej podpory, ktorú má verejný obstarávateľ uzavretú s výrobcom tretích strán. Pomôže s vytvorením ticketu a musí aktívne spolupracovať pri riešení, vyhodnocovaní vstupov ako aj celkovej interoperability riešenia.</li> <li>• možnosť otvorenia servisného prípadu bez nutnosti robiť vlastnú diagnostiku problému,</li> <li>• manažment servisného prípadu a koordinácia jednotlivých servisných tímov výrobcu musí byť zabezpečená výrobcom,</li> <li>• dostupnosť podporného centra v požadovanom režime 5x9 NBD, formou telefónu, mailu, portálu:</li> <li>• pre úroveň závažnosti incidentu kritická musí byť odpoveď Centra výrobcu do max. 1 hodina,</li> <li>• pre nižšiu ako kritickú úroveň závažnosti musí byť odpoveď Centra výrobcu v nasledujúci pracovný deň,</li> <li>• poskytovanie znalostnej bázy, obsahujúcej riešenia a odpovede na známe problémy, návody a postupy konfigurácie zariadení vo vzťahu v riešení</li> </ul> | <p>V rámci ponuky zabezpečíme servisnú podporu na obdobie 3 rokov od zakúpenia, ktorá plne spĺňa všetky požadované parametre:</p> <ul style="list-style-type: none"> <li>• V prípade poruchy zariadenia zabezpečíme jeho výmenu v režime Next Business Day (NBD) priamo v mieste prevádzky, čím sa minimalizuje doba výpadku.</li> <li>• Poskytovanie aktuálnych bezpečnostných záplat a hotfixov pre všetky produkty zahrnuté v dodanom riešení, s dôrazom na včasné reagovanie na nové bezpečnostné hrozby.</li> <li>• Pravidelné poskytovanie softvérových aktualizácií pre všetky produkty, vrátane zlepšení funkcionality a optimalizácie výkonu.</li> <li>• Zabezpečujeme komplexnú podporu pre celé riešenie, nielen pre jednotlivé produkty.</li> <li>• Podpora zahŕňa hardvérové aj softvérové komponenty od výrobcu, ktoré sú súčasťou nasadeného riešenia.</li> <li>• Podpora od výrobcu bude zahŕňať spoluprácu s tretími stranami v rámci platných podporných zmlúv.</li> <li>• Výrobca aktívne spolupracuje pri riešení incidentov s tretími stranami, vrátane pomoci pri zakladaní ticketov a zabezpečení hladkej interoperability riešenia.</li> <li>• Umožňujeme otvorenie servisného prípadu bez potreby predchádzajúcej diagnostiky zo strany zákazníka. Diagnostiku zabezpečí technický tím podpory.</li> <li>• Výrobca preberá zodpovednosť za kompletný manažment servisných prípadov vrátane koordinácie rôznych interných technických tímov.</li> <li>• Podporné centrum bude dostupné v režime 5x9 NBD prostredníctvom telefónu, e-mailu a webového portálu.</li> <li>• Pri kritických incidentoch: odpoveď do 1 hodiny.</li> <li>• Pri incidentoch s nižšou prioritou: odpoveď do nasledujúceho pracovného dňa.</li> <li>• Prístup k rozsiahlej znalostnej báze, ktorá obsahuje: <ul style="list-style-type: none"> <li>▪ riešenia známych problémov,</li> <li>▪ návody na konfiguráciu,</li> <li>▪ odporúčané postupy pre správu a optimalizáciu zariadení v rámci dodaného riešenia.</li> </ul> </li> </ul> |

## 2. Backup Firewall

Tabuľka č. 2

| Parameter:  | Minimálne požadované parametre:   | Hodnota:   | Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru   |
|---|---|--|--|
| <b>Systém pre zabezpečenie zálohovacích služieb SDDC prostredia formou Backup Firewall, poskytujúceho vlastnosti next-gen firewallu pre potreby vybudovania zabezpečeného VPN tunela medzi NCZI a SDDS prostredím.</b><br><i>Je nutné uviesť detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (Part Number, Product Code)</i> |   |  | <b>Backup Firewall od výrobcu Fortinet, Inc. s Product Code: FG-101F, ktorý bude obsahovať uvedenú detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (product code):</b><br><br><b>2x FG-101F</b><br><b>6x FC-10-F101F-928-02-12</b><br><br><a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf</a><br><br><a href="https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/954635/getting-started">https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/954635/getting-started</a><br><a href="https://docs.fortinet.com/product/fortigate/7.6">https://docs.fortinet.com/product/fortigate/7.6</a> |
| <b>Počet:</b>   | 2 ks<br>Dodané riešenie musí byť vo forme fyzických zariadení s výnimkou manažmentu riešenia, ktoré musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu. |  | v počte 2ks bude vo forme fyzických zariadení s výnimkou manažmentu riešenia, ktoré bude vo forme virtuálneho zariadenia pre virtualizačnú platformu.  |
| <b>Základné parametre</b>   | Priepustnosť Firewallu podľa RFC 3511, 2544, 2647, 1242   | Min. 18 Gb/s   | FG-101F dosahuje priepustnosť firewallu 18 Gb/s podľa RFC 3511, 2544, 2647, 1242.  |
|   | Priepustnosť IPS podľa RFC 3511, 2544, 2647, 1242   | Min. 2 Gb/s  | FG-101F poskytuje 2,6 Gb/s priepustnosť pre IPS podľa RFC 3511, 2544, 2647, 1242.  |
|   | Priepustnosť so zapnutou ochranou pred hrozbami (threat protection – antimalware, IPS, application control)   | Min. 1 Gb/s  | FG-101F dosahuje priepustnosť 1 Gb/s s aktívnou ochranou pred hrozbami so zapnutou ochranou pred hrozbami (threat protection – antimalware, IPS, application control).   |
|   | Priepustnosť IPsec VPN (512 bytes)  | Min. 11 Gb/s   | FG-101F dosahuje priepustnosť IPsec VPN 11,5 Gb/s (pri 512-bajtových paketoch).  |
|   | Priepustnosť SSL VPN  | Min. 1 Gb/s  | FG-101F dosahuje priepustnosť SSL VPN 1 Gb/s.  |
|   | Latencia (64 byte, UDP)   | Menej ako 5 mikrosekúnd (64 byte UDP)  | Latencia (64 byte, UDP) zariadenia FG-101F je 4,97 mikrosekundy.   |
|   | Počet nových spojení za sekundu (CPS)   | Min. 50 000  | Zariadenie FG-101F podporuje až 56 000 nových TCP spojení za sekundu.  |
|   | Počet súčasných spojení   | Min. 1 000 000   | FG-101F zvláda až 1,5 milióna súčasných spojení.   |
|   | Počet fyzických sieťových rozhraní  | Min. 10x GE RJ45<br>Min. 2x HA RJ45 port<br>Min. 2x 10 GE SFP+<br>Min. 4x GE SFP | má 12x GE RJ45 portov + 2x GE RJ45 MGMT/DMZ porty.<br>má 2x HA RJ45 port.<br>má 2x 10 GE SFP+ FortiLink.<br>má 4x GE SFP.  |
|   | Podpora virtuálnych domén / kontextov   | Min. 10  | FG-101F podporuje 10 virtuálnych domén (VDOMs)   |
| <b>Požadovaná funkcionálnosť</b>  | Podpora pre lokálne úložisko  | min. 480 GB  | FG-101F podporuje lokálne úložisko s kapacitou 480 GB.   |
|   | Podpora vysokej dostupnosti v konfigurácii Active-Passive, alebo Active-Active alebo Clustering   |  | FortiGate 101F podporuje vysokú dostupnosť (HA) v režimoch Active-Passive aj Active-Active, čo umožňuje nasadenie v klastroch pre zvýšenú spoľahlivosť a výkon.  |

|                         |  |  |
|-------------------------|--|--|
|                         | Podpora synchronizácie TCP, UDP spojení a sieťových prekladov  | FortiGate 101F podporuje synchronizáciu TCP, UDP spojení a sieťových prekladov.  |
|                         | Podpora Site to Site IPSEC tunelov.  | FortiGate 101F podporuje vytváranie IPsec VPN tunelov pre bezpečnú komunikáciu medzi rôznymi lokalitami.   |
|                         | Podpora 802.1Q VLAN, podpora 802.3ad pasívnej a aktívnej agregácie liniek.   | FortiGate 101F podporuje štandard 802.1Q pre VLAN trunking a tiež 802.3ad pre agregáciu liniek (LACP), čo umožňuje zvyšovať priepustnosť a redundanciu sieťových pripojení.  |
|                         | Firewall, IPS, Aplikačná kontrola, Malware a Botnet ochrana.   | S licenciou <b>FC-10-F101F-928-02-12</b> zariadenie FortiGate 101F poskytuje funkcie firewallu, systému prevencie prienikov (IPS), aplikačnej kontroly, ochrany pred malvérom a botnetmi.  |
|                         | Možnosť integrácie s externou Sandbox službou (cloud alebo on-premises).   | FortiGate 101F umožňuje integráciu s FortiSandbox pre pokročilú analýzu hrozieb, dostupnú ako cloudová služba alebo on-premises riešenie.  |
|                         | Musí realizovať filtrovanie tokov na základe doménovej / IP reputácie.   | FortiGate 101F využíva FortiGuard služby na hodnotenie reputácie domén a IP adries, čo umožňuje filtrovanie na základe týchto kritérií.  |
|                         | Musí podporovať filtrovanie web tokov na základe DNS requestov, url filtrovanie a blokovanie na známe botnet a C&C adresy  | FortiGate 101F poskytuje DNS filtrovanie, URL filtrovanie a ochranu proti botnetom prostredníctvom FortiGuard služieb, čo umožňuje blokovanie škodlivých adries a komunikácie s riadiacimi servermi.   |
|                         | Musí podporovať inšpekciu certifikátov počas SSL handshaku, bez potreby dešifrovania.  | FortiGate 101F podporuje inšpekciu SSL/TLS certifikátov počas handshaku, čo umožňuje overenie platnosti certifikátov bez úplného dešifrovania komunikácie.   |
|                         | Musí umožňovať filtrovanie na základe geografickej lokality.   | FortiGate 101F umožňuje filtrovanie a kontrolu prístupu na základe geografickej polohy IP adries, čo umožňuje obmedziť alebo povoliť prístup z konkrétnych regiónov.   |
|                         | Okamžite použiteľné preddefinované IPS politiky.   | FortiGate 101F obsahuje preddefinované politiky pre systém prevencie prienikov (IPS), ktoré sú okamžite použiteľné na ochranu siete pred známymi hrozbami.   |
|                         | Možnosť nastavenia monitorovacieho alebo blokovacieho režimu IPS globálne, na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry.  | Administrátori môžu konfigurovať IPS v monitorovacom (detekčnom) alebo blokovacom (preventívnom) režime na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry.   |
|                         | Automatické vypnutie IPS ochrany firewallu v prípade preťaženia  | FortiGate 101F je navrhnutý tak, aby v prípade preťaženia systému mohli upraviť alebo dočasne deaktivovať niektoré bezpečnostné funkcie, ako je IPS, aby sa zachovala základná funkčnosť siete.  |
|                         | Podpora pre grafické rozhranie cez HTML 5  | Webové administratívne rozhranie FortiGate 101F je založené na HTML5, čo umožňuje prístup a správu zariadenia prostredníctvom moderných webových prehliadačov bez potreby dodatočných pluginov.  |
| <b>Centrálna správa</b> | <ul style="list-style-type: none"> <li>Centrálny manažment musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu (minimálne podpora VMware ESXi).</li> <li>Musí podporovať správu min. 20 zariadení s možnosťou rozširovania pomocou licencie.</li> <li>Musí podporovať externé identity databázy vrátane LDAP databáz.</li> <li>Musí obsahovať intuitívne grafické rozhranie pre IPv4 klientov.</li> <li>Musí mať integrované monitorovacie, reportovacie aj diagnostické schopnosti pre maximálnu kontrolu a viditeľnosť.</li> <li>Podpora multitenantnosti – oddelené domény pre tenantov a role-based administratorké účty.</li> <li>Podpora automatizovaného REST API, skriptov.</li> <li>Podpora vysokej dostupnosti</li> </ul> | <ul style="list-style-type: none"> <li>Centrálny manažment je dostupný ako virtuálne zariadenie kompatibilné s rôznymi virtualizačnými platformami vrátane VMware ESXi.</li> <li>umožňuje správu min. 20 zariadení, pričom kapacitu je možné rozširovať prostredníctvom licencií podľa potrieb organizácie.</li> <li>podporuje integráciu s externými identitnými službami, vrátane LDAP, čo umožňuje centralizovanú správu užívateľov a autentifikáciu.</li> <li>poskytuje užívateľsky prívetivé grafické rozhranie pre IPv4 klientov založené na HTML5, ktoré je prístupné cez moderné webové prehliadače.</li> <li>obsahuje nástroje na monitorovanie siete, generovanie reportov a diagnostiku, čo poskytuje komplexný prehľad o stave siete a bezpečnostných udalostiach.</li> <li>Prostredníctvom administratívnych domén (ADOM) umožňuje</li> </ul> |

|                         |  |   |
|-------------------------|--|---|
|                         | <ul style="list-style-type: none"> <li>• Podpora pre zamknutie politik pre lepsiu kontrolu nad zmenami v multi admin prostredí.</li> <li>• Podpora pre automatické zálohovanie konfigurácií a sledovanie zmien pre audit.</li> <li>• Podpora pre centrálnu konfiguráciu pomocou šablátov.</li> <li>• Podpora centrálnej distribúcie signatúr.</li> <li>• Podpora viacerých správco a rôznych úrovni prístupových oprávnení.</li> <li>• Podpora odosielania logov na SYSLOG server.</li> <li>• Podpora viacerých administratívnych domén / tenantov</li> </ul>  | <p>oddelenú správu pre rôznych tenantov a podporuje role-based prístup pre administrátorov.</p> <ul style="list-style-type: none"> <li>• podporuje REST API a skriptovanie, čo umožňuje automatizáciu úloh a integráciu s inými systémami.</li> <li>• podporuje konfigurácie vysokej dostupnosti (HA) s automatickým prepnutím v prípade zlyhania, čím zabezpečuje nepretržitú prevádzku.</li> <li>• Funkcia uzamknutia politik umožňuje administrátorom kontrolovať a sledovať zmeny v prostredí s viacerými administrátormi, čím sa predchádza neúmyselným úpravám.</li> <li>• automaticky zálohuje konfigurácie zariadení a poskytuje revíziu históriu zmien pre účely auditu a obnovy.</li> <li>• Pomocou konfiguračných šablón umožňuje efektívne nasadzovať a spravovať nastavenia na viacerých zariadeniach súčasne.</li> <li>• umožňuje centralizovanú distribúciu bezpečnostných signatúr a aktualizácií na spravované zariadenia, čím zabezpečuje jednotnú úroveň ochrany.</li> <li>• Systém role-based prístupu umožňuje definovať rôzne úrovne oprávnení pre správco podľa ich úloh a zodpovedností.</li> <li>• podporuje export logov na externé SYSLOG servery pre centralizované ukladanie a analýzu.</li> <li>• Administratívne domény (ADOM) umožňujú segmentáciu správy pre rôznych tenantov alebo oddelenia v rámci jednej inštalácie</li> </ul> |
| <b>Záruka</b>           | <ul style="list-style-type: none"> <li>• záručná doba min. 3 roky</li> </ul>   | zariadenie Fortinet FortiGate 101F spĺňa požiadavky na záručnú dobu min. 3 roky.  |
|                         | <ul style="list-style-type: none"> <li>• spôsob servisu v mieste prevádzky, nonstop (8x5xNBD)</li> </ul>   | zariadenie Fortinet FortiGate 101F spĺňa požiadavky na spôsob servisu v mieste prevádzky v režime nonstop (8x5xNBD)   |
| <b>Inštalácia</b>       | <ul style="list-style-type: none"> <li>• súčasťou ponuky musí byť inštalačná služba obsahujúca dopravu, montáž, inštalácia a nastavenie dodaných zariadení prípadne softvérov, odskúšanie funkčnosti a prevádzkyschopnosti, uvedenie do prevádzky, zaškolenie kupujúcim určených osôb, vrátane inštalácie všetkých súčastí operačných prostredí.</li> <li>• inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného riešenia pre Backup firewall</li> <li>• uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané riešenie pre Backup firewall. (Poznámka: predmetný certifikát tvorí prílohu č. 5 ku kúpnej zmluve na predmet zákazky, uchádzač tento dokument nemusí predkladať vo svojej ponuke, postačuje, ak ho predloží úspešný uchádzač najneskôr pri podpise zmluvy).</li> </ul> | <ul style="list-style-type: none"> <li>• Súčasťou ponuky je komplexná inštalačná služba, ktorá zahŕňa zabezpečenie dopravy, fyzickú montáž, odbornú inštaláciu a konfiguráciu dodaných zariadení a softvéru. Táto služba zahŕňa aj testovanie funkčnosti a overenie prevádzkovej spoľahlivosti, uvedenie zariadení do plnej prevádzky a poskytnutie školenia pre určené osoby kupujúceho, vrátane nasadenia všetkých potrebných súčastí operačných systémov.</li> <li>• Inštalačné práce budú realizované kvalifikovaným odborníkom s platným certifikátom, ktorý ho oprávňuje vykonávať montáž, konfiguráciu a správu dodávaného riešenia určeného pre Backup firewall.</li> <li>• Ako uchádzač doložíme platný certifikát vydaný priamo výrobcom, producentom alebo autorizovanou osobou, ktorá má oprávnenie na vydávanie takýchto certifikátov pre riešenie súvisiace s Backup firewallom.</li> </ul>   |
| <b>Servisná podpora</b> | <ul style="list-style-type: none"> <li>• 3 roky od zakúpenia s nasledujúcimi parametrami:</li> <li>• výmena zariadenia v prípade poruchy (RMA) v režime nasledujúci pracovný deň v mieste prevádzky,</li> </ul>  | <p>V rámci ponuky zabezpečíme servisnú podporu na obdobie 3 rokov od zakúpenia, ktorá plne spĺňa všetky požadované parametre:</p> <ul style="list-style-type: none"> <li>• V prípade poruchy zariadenia zabezpečíme jeho výmenu v režime Next Business Day (NBD) priamo v mieste prevádzky, čím sa</li> </ul>   |



|  |   |   |
|--|---|---|
|  | <ul style="list-style-type: none"> <li>• včasné poskytovanie bezpečnostných záplat a hotfixov pre produkty v riešení,</li> <li>• poskytovanie softvérových aktualizácií pre produkty v riešení,</li> <li>• centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: <ul style="list-style-type: none"> <li>○ riešenie servisných prípadov na úrovni riešenia, nie len na úrovni podpory jednotlivých produktov,</li> <li>○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora,</li> <li>○ požaduje sa podpora od výrobcu s previazanosťou na produkty výrobcov tretích strán. Výrobca poskytne podporu pri riešení prípadu s iným výrobcom v rozsahu platnej podpory, ktorú má verejný obstarávateľ uzavretú s výrobcom tretích strán. Pomôže s vytvorením ticketu a musí aktívne spolupracovať pri riešení, vyhodnocovaní vstupov ako aj celkovej interoperabilite riešenia.</li> <li>○ možnosť otvorenia servisného prípadu bez nutnosti robiť vlastnú diagnostiku problému,</li> <li>○ manažment servisného prípadu a koordinácia jednotlivých servisných tímov výrobcu musí byť zabezpečená výrobcom,</li> <li>○ dostupnosť podporného centra v požadovanom režime 5x9 NBD, formou telefónu, mailu, portálu: <ul style="list-style-type: none"> <li>▪ pre úroveň závažnosti incidentu kritická musí byť odpoveď Centra výrobcu do max. 1 hodina,</li> <li>▪ pre nižšiu ako kritickú úroveň závažnosti musí byť odpoveď Centra výrobcu v nasledujúci pracovný deň,</li> </ul> </li> <li>○ poskytovanie znalostnej bázy, obsahujúcej riešenia a odpovede na známe problémy, návody a postupy konfigurácie zariadení vo vzťahu v riešení</li> </ul> </li> </ul> | <p>minimalizuje doba výpadku.</p> <ul style="list-style-type: none"> <li>• Poskytovanie aktuálnych bezpečnostných záplat a hotfixov pre všetky produkty zahrnuté v dodanom riešení, s dôrazom na včasné reagovanie na nové bezpečnostné hrozby.</li> <li>• Pravidelné poskytovanie softvérových aktualizácií pre všetky produkty, vrátane zlepšení funkcionality a optimalizácie výkonu.</li> <li>• Zabezpečujeme komplexnú podporu pre celé riešenie, nielen pre jednotlivé produkty.</li> <li>• Podpora zahŕňa hardvérové aj softvérové komponenty od výrobcu, ktoré sú súčasťou nasadeného riešenia.</li> <li>• Podpora od výrobcu bude zahŕňať spoluprácu s tretími stranami v rámci platných podporných zmlúv.</li> <li>• Výrobca aktívne spolupracuje pri riešení incidentov s tretími stranami, vrátane pomoci pri zakladaní ticketov a zabezpečení hladkej interoperability riešenia.</li> <li>• Umožňujeme otvorenie servisného prípadu bez potreby predchádzajúcej diagnostiky zo strany zákazníka. Diagnostiku zabezpečí technický tím podpory.</li> <li>• Výrobca preberá zodpovednosť za kompletný manažment servisných prípadov vrátane koordinácie rôznych interných technických tímov.</li> <li>• Podporné centrum bude dostupné v režime 5x9 NBD prostredníctvom telefónu, e-mailu a webového portálu.</li> <li>• Pri kritických incidentoch: odpoveď do 1 hodiny.</li> <li>• Pri incidentoch s nižšou prioritou: odpoveď do nasledujúceho pracovného dňa.</li> <li>• Prístup k rozsiahlej znalostnej báze, ktorá obsahuje: <ul style="list-style-type: none"> <li>▪ riešenia známych problémov,</li> <li>▪ návody na konfiguráciu,</li> <li>▪ odporúčané postupy pre správu a optimalizáciu zariadení v rámci dodaného riešenia.</li> </ul> </li> </ul> |
|--|---|---|

### 3. Centrálny systém SDDC firewallu

Tabuľka č. 3

| Parameter: | Minimálne požadované parametre:  | Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru  |
|------------|--|---|
|            |  | <p>Centrálny systém SDDC firewallu Maestro Hyperscale Network Security od výrobcu Check Point Software Technologies Ltd., ktorý bude obsahovať uvedenú detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (product code):</p> <p>2 ks CPAP-SG9400-SNBT<br/> 2 ks CPSB-NGFW-9400-2Y<br/> 2 ks CPAC-2-40/100F-D-INSTALL<br/> 2 ks CPSB-VS-25<br/> 2 ks CPAC-NLOM-D-INSTALL<br/> 2 ks CPAC-RAM48GB-9100/9400-INSTALL<br/> 1 ks CPAC-2-40/100F-D-INSTALL<br/> 1 ks CPAP-SG9400-SNBT<br/> 1 ks CPSB-VS-25<br/> 1 ks CPAC-NLOM-D-INSTALL<br/> 1 ks CPAC-RAM48GB-9100/9400-INSTALL</p> <p><a href="https://www.checkpoint.com/downloads/products/quantum-force-9400-datasheet.pdf">https://www.checkpoint.com/downloads/products/quantum-force-9400-datasheet.pdf</a></p> <p><a href="https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Gaia_AdminGuide/Content/Front-Matter/Important-Information-GAG.htm?tocpath=1">https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Gaia_AdminGuide/Content/Front-Matter/Important-Information-GAG.htm?tocpath=1</a></p> <p><a href="https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_VSX_AdminGuide/CP_R82_VSX_AdminGuide.pdf">https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_VSX_AdminGuide/CP_R82_VSX_AdminGuide.pdf</a></p> <p><a href="https://support.checkpoint.com/results/sk/sk181127">https://support.checkpoint.com/results/sk/sk181127</a></p> <p>1 ks CPAC-DAC-10G-3M-D<br/> 1 ks CPAC-DAC-10G-3M-D<br/> 1 ks CPSM-NGSM25-MD5<br/> 1 ks CPSB-EVS-25-2Y<br/> 1 ks CPSM-NGSM25-MD5</p> <p><a href="https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Multi-DomainSecurityManagement_AdminGuide/Content/Topics-MDSG/Getting-Started.htm">https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Multi-DomainSecurityManagement_AdminGuide/Content/Topics-MDSG/Getting-Started.htm</a></p> <p>4 ks CPAC-DAC-40G-3M-D<br/> 1 ks CPAC-DAC-40G-3M-D<br/> 4 ks CPAC-TR-100SR<br/> 1 ks CPAC-TR-100SR<br/> 2 ks CPAP-MHO-140<br/> 4 ks CPAC-TR-1T-D<br/> 1 ks CPAP-MHO-140<br/> 1 ks CPAC-TR-1T-D<br/> 2 ks CPSG-vSEC-ACI<br/> 1 ks CPSG-vSEC-ACI</p> <p><a href="https://www.checkpoint.com/downloads/products/maestro-hyperscale-orchestrator-datasheet.pdf">https://www.checkpoint.com/downloads/products/maestro-hyperscale-orchestrator-datasheet.pdf</a></p> <p><a href="https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Working-with-Maestro.htm?TocPath=Working%20with%20Quantum%20Maestro%20%7C0">https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Working-with-Maestro.htm?TocPath=Working%20with%20Quantum%20Maestro%20%7C0</a></p> |
|            | <p>Centrálny systém pre zabezpečenie služby interného SDDC firewallu, poskytujúceho vlastnosti next-gen firewallu pre potreby softvérovo definovanej sieťovej infraštruktúry (SDN).</p> <p><i>Je nutné uviesť detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (Part Number, Product Code)</i></p> |   |

|                  |   |   |
|------------------|---|---|
| Predmet dodania: | Centrálny systém SDDC firewallu predstavuje ucelený hyperškálovací systém alebo klaster, ktorý je tvorený dostatočným počtom a typmi zariadení pre spracovanie definovaného objemu prevádzky s požadovanými bezpečnostnými funkciami a vlastnosťami.  | Bude dodaný Centrálny systém SDDC firewallu <b>Maestro Hyperscale Network Security</b> , ktorý predstavuje ucelený hyperškálovací systém alebo klaster, ktorý je tvorený dostatočným počtom a typmi zariadení pre spracovanie definovaného objemu prevádzky s požadovanými bezpečnostnými funkciami a vlastnosťami.   |
| Počet:           | 1 ks – ucelený hyperškálovací systém alebo klaster, typy a počet zariadení tvoriacich systém má byť dostatočný na splnenie podmienok  | Systém <b>Maestro Hyperscale Network Security</b> je navrhnutý ako hyperškálovateľný klaster v počte 1ks s podporou, ktorý umožňuje zoskupenie viacerých zariadení do jedného výkonného celku. Konfigurácia zahŕňa dostatočný počet bezpečnostných brán a výkonových modulov, čím zabezpečuje splnenie požiadaviek na škálovanie a výkonnosť v prostredí SDDC.  |
| Požiadavky:      | <ul style="list-style-type: none"> <li>musí umožňovať efektívne škálovať a umožniť rozfázovanie jeho obstarania podľa reálnych požiadaviek prostredia Software-Defined Data Center (SDDC) <ul style="list-style-type: none"> <li>musí poskytovať výkon na úrovni min. 40 Gbps pre next generation funkcionality systému SDDC firewallu, podľa požiadaviek v časti „Technické vlastnosti“ (konfigurácia N)</li> <li>musí umožňovať rozšírenie výkonu na úroveň minimálne 80 Gbps pre next generation funkcionality systému SDDC firewallu, podľa požiadaviek v časti „Technické vlastnosti“ (konfigurácia N+1), z uvedeného dôvodu musí umožňovať efektívne škálovanie výkonu aj v budúcnosti, aby bol zabezpečený ďalší rozvoj a rast SDDC</li> </ul> </li> <li>musí byť navrhnutý modulárne, aby umožňoval jednoduché</li> </ul> | <ul style="list-style-type: none"> <li>Systém je navrhnutý s podporou hyperscale architektúry, ktorá umožňuje postupné rozfázovanie obstarania a škálovanie podľa aktuálnych potrieb SDDC. Pridávanie výkonových modulov a bezpečnostných brán umožňuje flexibilné rozširovanie systému v čase.</li> <li>Zariadenia v konfigurácii N poskytujú minimálny výkon 40 Gbps pre Next Generation Firewall (NGFW) funkcionality, čím zabezpečujú požadovanú úroveň ochrany a sieťového spracovania v prostredí SDDC.</li> <li>Systém umožňuje rozšírenie výkonu (konfigurácia N+1) na úroveň minimálne 80 Gbps prostredníctvom pridania ďalších zariadení a modulov do hyperscale klastru. Maestro Hyperscale Orchestrator zabezpečuje efektívne riadenie škálovania, čím sa umožňuje ďalší rast a rozvoj infraštruktúry v SDDC.</li> <li>Systém je modulárny a umožňuje jednoduché rozšírenie o dodatočné výkonnostné a sieťové moduly. Nové komponenty môžu byť pridané bez narušenia prevádzky.</li> <li>Systém podporuje vysokorychlostné sieťové rozhrania s možnosťou pripojenia 40 Gbps a 100 Gbps Ethernet portov, čím zaisťuje dostatočnú priepustnosť a výkon.</li> <li>Konfigurácia podporuje vysokú dostupnosť a redundanciu v režime (N+1). Maestro Hyperscale Orchestrator zabezpečuje automatické presmerovanie prevádzky a ochranu proti výpadkom jednotlivých zariadení.</li> <li>Systém umožňuje vytváranie virtuálnych inštancií firewallov a dynamické pridelovanie hardvérových zdrojov podľa aktuálnych potrieb prostredia SDDC, čím optimalizuje výkon a využitie dostupných prostriedkov.</li> <li>Nové zariadenia môžu byť jednoducho pridané do klastru vďaka automatickej konfigurácii riadenej systémom. Maestro Hyperscale Orchestrator zabezpečuje bezproblémovú integráciu nových komponentov bez nutnosti manuálneho zásahu.</li> <li>Systém podporuje rôzne modely bezpečnostných brán a firewallov v rámci jedného klastru, čo umožňuje budúcu integráciu nových zariadení výrobcu bez nutnosti výmeny pôvodných komponentov.</li> </ul> |

|                       |   |   |
|-----------------------|---|---|
|                       | <p>pridanie ďalších modulov alebo komponentov na zvýšenie výkonu</p> <ul style="list-style-type: none"> <li>• musí podporovať vysokorýchlostné sieťové rozhrania, vrátane 40 Gbps a 100 Gbps Ethernet portov</li> <li>• v konfigurácii (N+1) musí systém poskytovať vysokú dostupnosť a redundanciu tak, aby zabezpečil nepretržitú plnohodnotnú prevádzku aj v prípade zlyhania jedného zariadenia.</li> <li>• musí umožniť vytvárať virtuálne inštancie firewallov a dynamický presun HW zdrojov medzi nimi,</li> <li>• musí umožňovať jednoduché zaradenie nového zariadenia do systému / klastra pomocou automatickej konfigurácie systémom / klastrom,</li> <li>• podpora rozdielnych modelov dodávaného SDDC firewallu, ako napr. bezpečnostných brán / firewallov v rámci systému / klastra tak, aby bolo možné v budúcnosti integrovať nové modely výrobcu bez výmeny pôvodných zariadení,</li> </ul> |   |
| Technické vlastnosti: | <p>Systém musí na minimálne 36 mesiacov funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality:</p> <ul style="list-style-type: none"> <li>• plne automatizovaná infraštruktúra,</li> <li>• modulárna architektúra riešenia,</li> <li>• integrácia s centrálnym systémom softvérovo definovanej siete (SDN) od</li> </ul>  | <p>Systém bude minimálne 36 mesiacov funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality:</p> <ul style="list-style-type: none"> <li>• Systém podporuje plne automatizovanú infraštruktúru, umožňuje centralizovanú správu, dynamické škálovanie a automatické konfigurovanie komponentov v rámci hyperscale architektúry.</li> <li>• Riešenie je modulárne, umožňuje pridávanie výkonových, sieťových a bezpečnostných modulov bez nutnosti výmeny základnej infraštruktúry. Škálovateľnosť je zabezpečená pomocou hyperscale technológie.</li> <li>• Systém podporuje integráciu s CISCO ACI na úrovni dynamického získavania objektov a ich nasadzovania v bezpečnostných politikách, čím umožňuje efektívne riadenie bezpečnosti v SDN prostredí.</li> <li>• Bezpečnostné politiky sú automaticky aktualizované na základe dynamických objektov získavaných zo systému CISCO ACI, čím sa zabezpečuje presnosť a aktuálnosť politiky v reálnom čase.</li> <li>• Systém umožňuje automatickú aktualizáciu dynamických objektov bez manuálneho zásahu, čím minimalizuje potrebu administratívnych úkonov a zvyšuje bezpečnosť prostredia.</li> <li>• Systém umožňuje centralizovanú správu všetkých zariadení v klastri ako jeden objekt s jednotnou bezpečnostnou politikou.</li> </ul> |

|  |   |   |
|--|---|---|
|  | <p>výrobca Cisco – CISCO ACI, minimálne:</p> <ul style="list-style-type: none"> <li>○ dynamické získavanie objektov a ich použitie v bezpečnostných politikách,</li> <li>○ dynamické objekty sa musia aktualizovať automaticky bez potreby zásahu správcu.</li> </ul> <ul style="list-style-type: none"> <li>• správa všetkých dodaných hardvérových zariadení / firewallov v rámci konkrétneho klastra ako jeden objekt, s jednou politikou,</li> <li>• podpora vysokej dostupnosti vo forme A/A, A/S, klaster</li> <li>• spôsob nasadenia: Layer 2 (transparent), Layer 3 (routing) mode</li> <li>• podpora funkcií firewallu novej generácie (next-gen firewall / NGFW): <ul style="list-style-type: none"> <li>○ firewall, aplikačná inšpekcia / aplikačná kontrola, IPS, anti bot, Identity-based politiky, malware, botnet and zero-day ochrana,</li> <li>○ podpora pre: kontrolu prenášaných súborov pomocou on-prem sandboxu, URL filtering,</li> <li>○ detekcia a správa dátových súborov a typov na základe obsahu. Relevantný počet preddefinovaných typov údajov (min. 70). Možnosť vytvárať</li> </ul> </li> </ul> | <p>Využíva Maestro Hyperscale Orchestrator na jednotné riadenie a dynamické pridelovanie zdrojov.</p> <ul style="list-style-type: none"> <li>• Systém podporuje vysoko dostupné režimy Active/Active (A/A), Active/Standby (A/S) a Cluster Mode, čím zabezpečuje nepretržitú prevádzku a redundanciu v prípade výpadku komponentov.</li> <li>• Systém podporuje nasadenie v režime Layer 2 (transparentný mód) aj Layer 3 (routingový mód), čím umožňuje flexibilitu integráciu do rôznych sieťových infraštruktúr.</li> <li>• Systém poskytuje plnú funkcionality next-generation firewallu (NGFW) vrátane firewallovej ochrany, hlbokéj aplikačnej inšpekcie, prevencie narušenia (IPS), ochrany pred botnetmi a zero-day útokmi, ako aj identity-based politiky pre granularitu riadenia prístupu.</li> <li>• Systém podporuje on-prem sandboxing na analýzu súborov a blokovanie škodlivého obsahu ešte pred doručením používateľovi. Obsahuje URL filtering na kontrolu prístupu k webovým stránkam na základe kategorizácie a politiky organizácie.</li> <li>• Systém podporuje automatickú detekciu dátových súborov a klasifikáciu obsahu na základe kľúčových slov, regulárnych výrazov (regex), atribútov súborov a ďalších parametrov. Zahŕňa minimálne 70 preddefinovaných typov údajov a umožňuje vytváranie vlastných pravidiel.</li> <li>• Systém umožňuje konfiguráciu ako explicitný proxy server pre HTTP a HTTPS komunikáciu, čím poskytuje dodatočnú vrstvu zabezpečenia a kontroly nad webovou prevádzkou.</li> <li>• Systém dokáže získavať identity používateľov priamo z Active Directory (AD) bez nutnosti inštalácie softvéru na AD servery. Identita používateľa sa môže zdieľať medzi viacerými firewallmi bez potreby externých autentifikačných komponentov.</li> <li>• Systém môže používať behaviorálnu analýzu a sandboxing na detekciu a blokovanie prvého pokusu o stiahnutie neznámeho alebo zero-day malvéru pred jeho vykonaním na koncovom zariadení.</li> <li>• Systém umožňuje manuálne aj automatizované pridanie IOC (Indicators of Compromise), vrátane IP adries, MD5 hashov a URL adries, a to buď cez administrátorské rozhranie alebo cez REST API integráciu.</li> <li>• Systém v základnej konfigurácii (N) poskytuje minimálne 40 Gbps výkonu pre next-generation firewall (NGFW) funkcionality, čím spĺňa požiadavky na zabezpečenie SDCC prostredia.</li> <li>• Systém umožňuje rozšírenie výkonu na minimálne 80 Gbps v konfigurácii (N+1) pridaním ďalších bezpečnostných zariadení do hyperscale klastra, čím sa zabezpečuje vyššia priepustnosť a odolnosť proti výpadkom.</li> <li>• Riešenie podporuje lineárne škálovanie výkonu pri pridaní ďalších zariadení do hyperscale klastra, pričom nie je potrebná výmena existujúceho hardvéru. Maestro Hyperscale Orchestrator umožňuje plynulú integráciu nových komponentov bez narušenia prevádzky.</li> <li>• Systém podporuje hot-swap pripojenie nových zariadení do klastra bez potreby výpadku služieb alebo zásahov do existujúcej sieťovej infraštruktúry na úrovni Layer 2 (L2) a Layer 3 (L3).</li> <li>• Maestro Hyperscale Orchestrator automaticky rozkladá zaťaženie medzi jednotlivé zariadenia v klastri, čím zabezpečuje optimálne využitie výpočtových a sieťových zdrojov v rámci celého riešenia.</li> <li>• Systém umožňuje automatickú synchronizáciu stavových informácií medzi jednotlivými členmi klastra, čím sa zabezpečuje kontinuita prevádzky a vysoká dostupnosť aj v prípade výpadku jednej zo súčastí riešenia.</li> <li>• Systém umožňuje prevádzku minimálne 25 virtuálnych inštancií firewallu (VSX / Virtual Systems), čím spĺňa požiadavky na oddelenie a segmentáciu bezpečnostných politík v prostredí SDCC.</li> <li>• Riešenie umožňuje dynamické pridanie ďalších virtuálnych inštancií firewallu prostredníctvom licenčného rozšírenia, bez potreby výmeny hardvéru alebo výpadku prevádzky.</li> <li>• Systém podporuje active/active (A/A) architektúru, v ktorej všetky hardvérové zariadenia v klastri aktívne spracovávajú prevádzku pre každú povolenú virtuálnu inštanciu firewallu. Maestro Hyperscale Orchestrator zabezpečuje automatické rozloženie záťaže medzi všetky zariadenia v klastri.</li> <li>• Riešenie podporuje plnú integráciu s Cisco ACI vo forme virtualizácie sieťových služieb (NFV). Virtuálne inštancie firewallu môžu byť dynamicky nasadené a riadené prostredníctvom SDN, s možnosťou využitia dynamických bezpečnostných politík a automatizovaného riadenia prevádzky.</li> <li>• Systém podporuje minimálne 5 nezávislých tenantov, pričom každý tenant má vlastné bezpečnostné politiky, konfigurácie a zdroje v rámci SDN prostredia.</li> <li>• Riešenie umožňuje dynamické pridanie ďalších tenantov prostredníctvom rozšírenia licencie, bez potreby výpadku služieb alebo zásahov do existujúcej infraštruktúry.</li> <li>• Každý tenant má samostatnú správu a konfiguráciu, pričom je zabezpečené úplné oddelenie administrácie a politik medzi</li> </ul> |
|--|---|---|

|  |  |  |
|--|--|--|
|  | <p>vlastné typy údajov na základe kľúčových slov, regexov, atribútov súborov a iných,</p> <ul style="list-style-type: none"> <li>o podpora pre explicitné HTTP / HTTPS proxy</li> <li>o možnosť získať používateľské identity z AD bez inštalácie software na AD servery. Zdieľanie identít medzi FW bez potreby externých komponentov,</li> <li>o blokovanie prvého pokusu o stiahnutie malvéru zero-day,</li> <li>o pridanie vlastných indikátorov IOC (IP, MD5, URL), manuálne alebo prostredníctvom API,</li> </ul> <ul style="list-style-type: none"> <li>• výkon, škálovanie a konektivita riešenia: <ul style="list-style-type: none"> <li>o minimálne 40 Gbps (konfigurácia N)</li> <li>o minimálne 80 Gbps (konfigurácia N+1)</li> <li>o možnosť škálovať výkon vyššie v prípade budúcej potreby, lineárny nárast výkonu pri pridaní ďalších zariadení, bez výmeny existujúceho hardvéru</li> <li>o pridanie ďalších hardvérových zariadení bez výpadku služieb a bez zmien infraštruktúry L2/L3 (hot-swap),</li> <li>o rozkladanie zaťaženia použitých hardvérových zariadení interne v rámci riešenia,</li> </ul> </li> </ul> | <p>jednotlivými tenantmi v rámci SDN prostredia.</p> <ul style="list-style-type: none"> <li>• Systém poskytuje role-based access control (RBAC), umožňujúci detailné pridelovanie oprávnení pre jednotlivých administrátorov v rámci rôznych tenantov.</li> <li>• Riešenie podporuje REST API pre integráciu s automatizačnými a orchestračnými nástrojmi, vrátane Ansible, Terraform/OpenTOFU a ďalších. API umožňuje plnú správu konfigurácie, politik a dynamické škálovanie firewallových inštancií a bezpečnostných pravidiel.</li> </ul> |
|--|--|--|

|  |   |  |
|--|---|--|
|  | <ul style="list-style-type: none"> <li>○ synchronizácia stavových informácií medzi jednotlivými členmi klastra,</li> <li>• podpora min. 25 inštancií virtuálnych inštancií firewallu, <ul style="list-style-type: none"> <li>○ možnosť pridať ďalšie inštancie (zmenou / doplnením licencie) vo fáze prevádzky,</li> <li>○ systém musí byť schopný spracovať prevádzku pre každú virtuálnu inštanciu pomocou každého dostupného hardvérového zariadenia, vytvárajúceho active / active klaster. Každé priradené hardvérové zariadenie sa musí aktívne podieľať na spracovaní prevádzky pre každú povolenú virtuálnu inštanciu (A/A).</li> <li>○ možnosť plne integrovať virtuálne inštancie firewallov do navrhovanej SDN od výrobcu Cisco – CISCO ACI vo forme virtualizácie sieťových služieb (Network functions virtualization / NFV),</li> </ul> </li> <li>• podpora ochrany multitenantnej prevádzky / viacerých tenantov v rámci SDN: <ul style="list-style-type: none"> <li>○ v počte min. 5 tenantov,</li> <li>○ možnosť pridať ďalšie tenanty (zmenou /</li> </ul> </li> </ul> |  |
|--|---|--|

|                           |   |   |
|---------------------------|---|---|
|                           | <p>doplnením licencie)<br/>počas prevádzky,</p> <ul style="list-style-type: none"> <li>o oddelenie manažmentu jednotlivých tenantov,</li> <li>o podpora RBAC</li> <li>• REST API pre integráciu s automatizačnými a orchestračnými systémami nástrojmi (ako napr.: Ansible, Terraform/OpenTOFU, ...),</li> </ul>  |   |
| Centrálna správa riešenia | <ul style="list-style-type: none"> <li>• Oddelená jednotná centrálna správa riešenia na virtuálnom alebo hardvérovom zariadení, s podporou: <ul style="list-style-type: none"> <li>o správy konfigurácií, politík a analýzy logov,</li> <li>o správy a prevádzky navrhovaného počtu tenantov,</li> <li>o správy a prevádzky navrhovaného počtu virtuálnych inštancií firewallu,</li> <li>o kontrola politík na duplicitu a nekonzistencie pred nasadením,</li> </ul> </li> <li>• centralizovaný zber, spracovanie a možnosť lokálnej analýzy logov,</li> <li>• integrácia do existujúceho Centrálného bezpečnostného, logovacieho a vyhodnocovacieho nástroja, zloženého z technológií: <ul style="list-style-type: none"> <li>o IBM QRadar 7.5</li> <li>o The Hive Project 4</li> <li>o MISP</li> <li>o Greycortex Mendel</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Systém poskytuje centrálnu správu konfigurácií, bezpečnostných politík a analýzy logov prostredníctvom dedikovaného manažmentového riešenia, ktoré môže byť nasadené ako virtuálne alebo hardvérové zariadenie.</li> <li>• Centrálna správa umožňuje riadenie a prevádzku všetkých tenantov, pričom každý tenant môže mať vlastné bezpečnostné politiky, nastavenia a administrátorov v rámci multitenantného prostredia.</li> <li>• Centrálna správa podporuje komplexnú správu všetkých virtuálnych firewallových inštancií vrátane ich nasadenia, monitorovania výkonu a dynamického pridelovania zdrojov v rámci SDN.</li> <li>• Systém obsahuje automatizovaný mechanizmus na kontrolu bezpečnostných politík, ktorý dokáže identifikovať duplicitu, konflikty a nekonzistencie pred ich nasadením, čím sa minimalizuje riziko chýb a zabezpečuje konzistentnosť politík.</li> <li>• Systém podporuje centralizovaný zber, spracovanie a analýzu logov s možnosťou lokálneho ukladania a vyhodnocovania údajov. Logy môžu byť spracovávané priamo v manažmentovej platforme alebo exportované do externých systémov na ďalšiu analýzu.</li> <li>• Systém podporuje natívnu integráciu s IBM QRadar 7.5 prostredníctvom Syslog, LEEF a API, čo umožňuje efektívne spracovanie bezpečnostných udalostí a forenznú analýzu.</li> <li>• Systém podporuje automatické posielania incidentov a hrozieb do The Hive Project 4 cez REST API alebo Syslog. Umožňuje koreláciu bezpečnostných udalostí a ich spracovanie v rámci existujúceho incident response workflow.</li> <li>• Systém podporuje integráciu so systémom MISP (Malware Information Sharing Platform) na zdieľanie a získavanie threat intelligence dát. Možnosť manuálneho aj automatizovaného importu IoC (Indicators of Compromise) a ich aplikácie v bezpečnostných politikách.</li> <li>• Systém umožňuje export logov a sieťových udalostí do Greycortex Mendel na pokročilú analýzu sieťovej prevádzky a detekciu anomálií. Podpora štandardných logovacích protokolov vrátane Syslog a NetFlow/IPFIX.</li> </ul> |



|   |  |  |
|---|--|--|
| Počet zariadení / vysoká dostupnosť riešenia: | <ul style="list-style-type: none"> <li>systém musí byť plnohodnotne redundantný a vysoko dostupný,</li> <li>konfigurácia počtu bezpečnostných zariadení: <ul style="list-style-type: none"> <li>podľa požiadavky na výkon - typu N</li> <li>podľa požiadavky na výkon - typu N+1</li> </ul> </li> </ul>                          | <ul style="list-style-type: none"> <li>Riešenie podporuje plnú redundanciu a vysokú dostupnosť prostredníctvom Active/Active (A/A) alebo Active/Standby (A/S) konfigurácie. Maestro Hyperscale Orchestrator zabezpečuje dynamické rozloženie záťaže a prevádzku bez výpadkov aj pri zlyhaní jednotlivých zariadení.</li> <li>Systém v konfigurácii N poskytuje minimálny výkon 40 Gbps, pričom počet bezpečnostných zariadení je optimalizovaný na splnenie tejto požiadavky.</li> <li>Systém v konfigurácii N+1 poskytuje minimálny výkon 80 Gbps, pričom umožňuje pridanie ďalších zariadení pre zvýšenie kapacity a zabezpečenie redundancie. Riešenie podporuje automatické vyvažovanie záťaže a bezvýpadkové pridanie nových zariadení (hot-swap).</li> </ul> |
| Sieťová konektivita                           | <ul style="list-style-type: none"> <li>konektivita do SDN prostredia: <ul style="list-style-type: none"> <li>agregované, plne redundantné externé uplinky do infraštruktúry, do každého LEAF prepínača infraštruktúry</li> <li>požadované: 4x 100GBASE SR4 porty pre vysokorýchlostné sieťové pripojenia</li> </ul> </li> </ul>  | <ul style="list-style-type: none"> <li>Systém podporuje plnú integráciu do SDN prostredia, pričom umožňuje dynamické riadenie sieťovej prevádzky a aplikáciu bezpečnostných politík v rámci softvérovo definovanej siete.</li> <li>Systém poskytuje agregované a plne redundantné uplinky s podporou vysokej dostupnosti, pričom zabezpečuje nepretržitú konektivitu ku každému LEAF prepínaču v SDN infraštruktúre.</li> <li>Riešenie obsahuje minimálne 4x 100GBASE SR4 porty, ktoré umožňujú vysokorýchlostné sieťové pripojenia s vysokou priepustnosťou a nízkou latenciou, čím sa zabezpečuje bezproblémová komunikácia v rámci SDN infraštruktúry.</li> </ul>   |
| Požiadavky na jednotlivé zariadenia:          |  |  |
| Napájacie zdroje                              | <ul style="list-style-type: none"> <li>redundantné (redundancia 1+1),</li> <li>maximálny výkon jedného zdroja 350W pri 230V</li> </ul>   | <ul style="list-style-type: none"> <li>Systém je vybavený dvojicou redundantných napájacích zdrojov v konfigurácii 1+1, čo zabezpečuje nepretržitú prevádzku aj v prípade zlyhania jedného zdroja.</li> <li>Používané napájacie zdroje majú maximálny výkon 350W pri 230V, čím spĺňajú požiadavky na energetickú efektivitu a stabilitu napájania.</li> </ul>  |
| Prevedenie                                    | <ul style="list-style-type: none"> <li>19" serverová skriňa</li> <li>maximálna výška 1RU per zariadenie</li> </ul>   | <ul style="list-style-type: none"> <li>Systém je navrhnutý pre štandardnú 19" serverovú skriňu, čím je zabezpečená kompatibilita s existujúcou rackovou infraštruktúrou.</li> <li>Každé zariadenie má maximálnu výšku 1RU, čo umožňuje efektívne využitie priestoru v serverovej skrini a optimalizáciu hustoty nasadenia.</li> </ul>  |
| OOB správa:                                   | <ul style="list-style-type: none"> <li>každé hardvérové zariadenie musí byť vybavené samostatným Lights Out Management (LOM) interface pre vzdialenú správu a monitorovanie. Tento interface musí umožniť správu zariadenia aj v prípade, že je zariadenie vypnuté alebo sa nachádza v stave nízkej spotreby energie.</li> </ul> | <p>Každé zariadenie obsahuje dedikovaný LOM (Lights Out Management) interface, ktorý umožňuje nezávislú vzdialenú správu a dohľad nad zariadením bez ohľadu na jeho prevádzkový stav. LOM interface podporuje správu zariadenia aj pri jeho vypnutí alebo v režime nízkej spotreby, čo umožňuje vzdialené zapnutie, diagnostiku a rekonfiguráciu bez fyzického prístupu k zariadeniu.</p>  |
| Servisná podpora                              | 3 roky od zakúpenia s nasledujúcimi  | <p>Bude zabezpečená servisná podpora na obdobie 3 roky od zakúpenia s nasledujúcimi parametrami:</p> <ul style="list-style-type: none"> <li>Systémová podpora zahŕňa výmenu zariadenia v prípade poruchy v režime 8 hodín denne, 5 dní v týždni s dodaním náhradného</li> </ul>  |

|  |   |  |
|--|---|--|
|  | <p>parametrami:</p> <ul style="list-style-type: none"> <li>výmena zariadenia v prípade poruchy v režime 8x5xNBD,</li> <li>včasné poskytovanie bezpečnostných záplat a hot-fixov pre produkty v riešení,</li> <li>poskytovanie softvérových aktualizácií pre produkty v riešení,</li> <li>centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: <ul style="list-style-type: none"> <li>riešenie servisných prípadov na úrovni riešenia, nie len na úrovni podpory jednotlivých produktov,</li> <li>podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora,</li> <li>požaduje sa podpora od výrobcu s previazanosťou na produkty výrobcov tretích strán minimálne Cisco (ACI). Výrobca poskytne podporu pri riešení prípadu s iným výrobcom v rozsahu platnej podpory, ktorú má verejný obstarávateľ uzavretú s výrobcom tretích strán. Pomôže s vytvorením ticketu a musí aktívne spolupracovať pri riešení, vyhodnocovaní vstupov ako aj celkovej interoperabilite riešenia.</li> <li>možnosť otvorenia servisného prípadu bez nutnosti robiť vlastnú diagnostiku problému,</li> <li>manažment servisného prípadu a koordinácia jednotlivých</li> </ul> </li> </ul> | <p>zariadenia na nasledujúci pracovný deň (NBD – Next Business Day).</p> <ul style="list-style-type: none"> <li>Výrobca poskytuje pravidelné bezpečnostné aktualizácie a hot-fixy, ktoré zabezpečujú okamžitú reakciu na nové hrozby a zraniteľnosti.</li> <li>Súčasťou podpory je prístup k softvérovým aktualizáciám vrátane nových funkcionalít, opráv chýb a bezpečnostných vylepšení počas celého obdobia podpory.</li> <li>Výrobca poskytuje komplexnú podporu celého riešenia, pričom sa servisné prípady riešia z pohľadu celkovej funkcionality systému, nie izolovane pre jednotlivé komponenty.</li> <li>Poskytovaná je kompletná podpora hardvérových aj softvérových produktov, vrátane ich integrácie a prevádzky v rámci dodaného riešenia.</li> <li>Výrobca poskytuje podporu pri riešení servisných prípadov súvisiacich s interoperabilitou Cisco ACI. Pomáha s vytvorením ticketu a aktívne spolupracuje pri diagnostike a riešení problémov v rámci kompatibility so systémami tretích strán.</li> <li>Používateľ môže otvoriť servisný prípad bez nutnosti predchádzajúcej diagnostiky, výrobca zabezpečuje analýzu problému a odporúčenie riešenia.</li> <li>Výrobca zabezpečuje manažment celého servisného prípadu, vrátane koordinácie tímov technickej podpory a eskalácie na vyššiu úroveň podpory, ak je to potrebné.</li> <li>Podporné centrum je dostupné 5 dní v týždni, 9 hodín denne, pričom používateľ môže kontaktovať podporu telefonicky, e-mailom alebo prostredníctvom online portálu.</li> <li>Pri kritických incidentoch je reakčný čas výrobcu garantovaný do 30 minút, čo umožňuje rýchle riešenie bezpečnostných alebo prevádzkových problémov.</li> <li>Pri menej závažných incidentoch je odpoveď garantovaná do 4 hodín alebo najneskôr v nasledujúci pracovný deň, čo umožňuje efektívne riešenie menej urgentných problémov.</li> <li>Používateľ má prístup k znalostnej báze výrobcu, ktorá obsahuje riešenia a odpovede na známe problémy, návody na konfiguráciu zariadení a osvedčené postupy pre správu a optimalizáciu riešenia.</li> </ul> |
|--|---|--|

|            |  |   |
|------------|--|---|
|            | <p>servisných tímov výrobcu musí byť zabezpečená výrobcom,</p> <ul style="list-style-type: none"> <li>o dostupnosť podporného centra v požadovanom režime 5x9 NBD, formou telefónu, mailu, portálu: <ul style="list-style-type: none"> <li>▪ pre úroveň závažnosti incidentu kritická musí byť odpoveď Centra výrobcu do max. 30min,</li> <li>▪ pre nižšiu ako kritickú úroveň závažnosti musí byť odpoveď Centra výrobcu do max. 4h alebo v nasledujúci pracovný deň,</li> </ul> </li> <li>o poskytovanie znalostnej bázy, obsahujúcej riešenia a odpovede na známe problémy, návody a postupy konfigurácie zariadení vo vzťahu v riešení</li> </ul>  |   |
| Inštalácia | <ul style="list-style-type: none"> <li>• súčasťou ponuky musí byť inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie dodaných zariadení prípadne softvérov pre preukázanie funkčnosti a prevádzkyschopnosti dodaného riešenia,</li> <li>• inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného riešenia,</li> <li>• uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávaný systém SDDC firewallu (Poznámka: predmetný certifikát tvorí prílohu č. 6 ku kúpnej zmluve na predmet zákazky, uchádzač tento dokument</li> </ul> | <ul style="list-style-type: none"> <li>• Inštalačné služby sú súčasťou ponuky a zahŕňajú dopravu, montáž, inštaláciu a nastavenie hardvérových zariadení a softvérových komponentov s cieľom preukázať ich plnú funkčnosť a prevádzkyschopnosť.</li> <li>• Inštaláciu (montáž, inštaláciu a nastavenie) vykonajú certifikovaní odborníci, ktorí sú oprávnení realizovať montáž, konfiguráciu a nasadenie dodávaného riešenia v súlade s požiadavkami výrobcu.</li> <li>• Uchádzač disponuje platným certifikátom výrobcu alebo oprávnenej osoby pre inštaláciu a konfiguráciu SDDC firewall riešenia. Tento certifikát bude predložený najneskôr pri podpise zmluvy v súlade s podmienkami obstarávania.</li> </ul> |

|  |   |  |
|--|---|--|
|  | nemusí predkladať vo svojej ponuke, postačuje, ak ho predloží úspešný uchádzač najneskôr pri podpise zmluvy). |  |
|--|---|--|

#### 4. Emailová brána

Tabuľka č. 4

| Parameter:            | Minimálne požadované parametre:  | Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru  |
|-----------------------|--|---|
|                       | Emailová brána zabezpečuje komplexnú ochranu e-mailovej komunikácie organizácie pred rôznymi bezpečnostnými hrozbami, ako sú škodlivé útoky, phishing, spam a pokročilé hrozby.<br><i>Je nutné uviesť detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (Part Number, Product Code)</i> | Emailová brána od výrobcu Fortinet, Inc. s Product Code: FML-VM02, ktorá bude obsahovať uvedenú detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (product code):<br><br>1x FML-VM02<br>3x FC-10-0VM02-642-02-12<br><br><a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf</a><br><br><a href="https://docs.fortinet.com/document/fortimail/7.4.3/administration-guide/347528">https://docs.fortinet.com/document/fortimail/7.4.3/administration-guide/347528</a> |
| Počet:                | 1 ks, ktorý musí byť dodaný vo forme virtuálneho zariadenia pre virtualizačnú platformu.   | Dodané riešenie v počte 1ks bude vo forme virtuálneho zariadenia pre virtualizačnú platformu.   |
| Základné parametre    | Email routing (messages / hod.) – min. 65000   | FML-VM02 dosahuje priepustnosť 67 000 správ za hodinu   |
|                       | Antispam + Antivirus (messages / hod.) – min. 50000  | FML-VM02 spracováva 54 000 správ za hodinu s aktívnymi funkciami antispamu a antivírusu.  |
|                       | Počet chránených domén – 70  | FML-VM02 podporuje 70 chránených e-mailových domén.   |
|                       | Vysoká dostupnosť - možnosť vysokej dostupnosti: active-passive alebo active-active.   | FML-VM02 podporuje konfigurácie vysokej dostupnosti (HA) v režimoch active-passive aj active-active.  |
|                       | Platforma - Dodané riešenie musí byť vo forme virtuálneho zariadenia.  | FML-VM02 bude dodané vo forme virtuálneho zariadenia.   |
|                       | Virtuálne zariadenie musí podporovať hypervizorové platformy: ako napr.: VMware, Citrix XenServer, Hyper-V, KVM, ...   | FML-VM02 podporuje hypervizory vrátane VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer a KVM.  |
|                       | Počet virtuálnych sieťových rozhraní – podpora pre min. 4 sieťové rozhrania  | FML-VM02 podporuje 4 virtuálne sieťové rozhrania.   |
|                       | Podpora pre lokálne úložisko – min. 2 TB   | FML-VM02 podporuje 2 TB virtuálneho úložiska.   |
|                       | Podpora pre grafické rozhranie cez HTML 5  | FML-VM02 poskytuje webové grafické rozhranie založené na HTML5.   |
| Základná funkcionálna | Podpora pre Advanced Multi-Layer Malware protection  | FML-VM02 poskytuje pokročilú viacvrstvovú ochranu proti malvéru (Advanced Multi-Layer Malware protection), vrátane antispamu, antivírusu, analýzy správania a sandboxingu.  |
|                       | Integrácia s LDAP serverom   | FML-VM02 podporuje integráciu s LDAP pre overovanie používateľov, smerovanie e-mailov a per-user inšpekciu pomocou LDAP atribútov.  |
|                       | Podpora pre secure message delivery (TLS)  | FML-VM02 podporuje bezpečné doručovanie správ pomocou TLS na zabezpečenie šifrovaného prenosu e-mailov.   |
|                       | Podpora Identity Based encryption  | FML-VM02 poskytuje Identity-Based Encryption (IBE) pre bezpečné šifrovanie e-mailov bez potreby predchádzajúcej výmeny kľúčov.  |
|                       | Podpora SMTP autentizácie cez LDAP, RADIUS, POP3 a IMAP  | FML-VM02 umožňuje SMTP autentizáciu prostredníctvom LDAP, RADIUS, POP3 a IMAP protokolov.   |
|                       | Podpora pre role-based / per-doména administrátorské účty  | FML-VM02 podporuje role-based a per-doména administrátorské účty pre granulárnu správu prístupu a oprávnení.  |
|                       | Logovanie a reportovanie aktivít a konfiguračných zmien  | FML-VM02 poskytuje podrobné logovanie a reportovanie aktivít, vrátane konfiguračných zmien, čo umožňuje sledovanie a auditovanie systému.   |
|                       | Per user inšpekcia pomocou LDAP atribútov  | FML-VM02 umožňuje per-user inšpekciu e-mailov na základe LDAP   |

|                   |  |   |
|-------------------|--|---|
|                   |  | atribútov, čo umožňuje prispôsobenie bezpečnostných politík pre jednotlivých používateľov.  |
|                   | Podpora pre Geo IP politiky  | FML-VM02 podporuje Geo IP politiky, čo umožňuje filtrovanie e-mailov na základe geografického pôvodu IP adresy odosielateľa.  |
|                   | Podpora pre skenovanie PDF a analýza obrázkov  | FML-VM02 poskytuje skenovanie PDF súborov a analýzu obrázkov na detekciu skrytého malvéru alebo nevhodného obsahu.  |
|                   | Podpora S/MIME   | FML-VM02 podporuje S/MIME pre digitálne podpisovanie a šifrovanie e-mailov, čím zabezpečuje integritu a dôvernosť komunikácie.  |
|                   | Podpora Greylistingu pre IPv4 a IPv6.  | FML-VM02 implementuje greylisting pre IPv4 aj IPv6 adresy na zníženie množstva spamu prijatého z neznámych zdrojov.   |
|                   | Podpora integrácie s third-party spam URI  | FML-VM02 umožňuje integráciu s tretími stranami poskytujúcimi spam URI zoznamy na zlepšenie detekcie a blokovania spamových správ.  |
|                   | Podpora pre Exchange journal archiving   | FML-VM02 podporuje archiváciu denníkov (journal archiving) z Microsoft Exchange, čo umožňuje uchovávanie kópií všetkých e-mailových komunikácií pre účely archivácie a súladu s predpismi.  |
|                   | Podpora pre enterprise identity štandardy (SPF, DKIM, DMARC)   | FML-VM02 podporuje štandardy SPF, DKIM a DMARC na overovanie identity odosielateľov a ochranu proti spoofingu a phishingovým útokom.  |
| <b>Záruka</b>     | záručná doba min. 2 roky<br>spôsob servisu: v mieste prevádzky, nonstop (24x7x365) s reakčnou dobou 4 hodiny a dobou opravy do 24 hodín.   | FML-VM02 spĺňa požiadavky na záručnú dobu min. 2 roky.<br>a spĺňa požiadavky na spôsob servisu v mieste prevádzky v režime nonstop (24x7x365) s reakčnou dobou 4 hodiny a dobou opravy do 24 hodín.   |
| <b>Inštalácia</b> | súčasťou ponuky musí byť inštalačná služba obsahujúca dodávku, inštaláciu a nastavenie dodaných softvérov, odskúšanie funkčnosti a prevádzkyschopnosti, uvedenie do prevádzky, zaškolenie kupujúcim určených osôb, vrátane inštalácie všetkých súčastí operačných prostredí. | Súčasťou ponuky je komplexná inštalačná služba, ktorá zahŕňa zabezpečenie dodávky, dopravy, odbornú inštaláciu a konfiguráciu dodaných softvérov. Táto služba zahŕňa aj testovanie funkčnosti a overenie prevádzkovej spoľahlivosti, uvedenie do plnej prevádzky a poskytnutie školenia pre určené osoby kupujúceho, vrátane nasadenia všetkých potrebných súčastí operačných systémov. |

## 5. PAM Server

Tabuľka č. 5

| Parameter:  | Minimálne požadované parametre:  | Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru  |
|---|--|---|
| Privileged Access Management (PAM) server zabezpečuje centralizovanú správu a ochranu privilegovaných účtov a prístupov v rámci organizácie.<br><i>Je nutné uviesť detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (Part Number, Product Code)</i> |  | PAM Server od výrobcu Fortinet, Inc. FortiPAM (Privileged Access Management) s Product Code: FC4-10-PAVUL-591-02-36, ktorá bude obsahovať uvedenú detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (product code):<br>FortiPAM pozostáva z Product Code: 50x FC4-10-PAVUL-591-02-36<br><a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortipam.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortipam.pdf</a><br><a href="https://docs2.fortinet.com/document/fortipam/1.5.0/administration-guide/790096">https://docs2.fortinet.com/document/fortipam/1.5.0/administration-guide/790096</a>   |
| Počet:  | 1 ks, ktorý musí byť dodaný vo forme virtuálneho zariadenia pre virtualizačnú platformu.   | v počte 1ks bude vo forme virtuálneho zariadenia pre virtualizačnú platformu.   |
| Vysoká dostupnosť   | Musí podporovať vysokú dostupnosť.   | FortiPAM podporuje vysokú dostupnosť (HA) prostredníctvom konfigurácie Active-Passive klastrov.   |
| Základná funkcionality  | <ul style="list-style-type: none"> <li>Musí mať možnosť obsluhovať min. 50 používateľov.</li> <li>Musí podporovať multi-faktorovú autentizáciu vo forme tokenu v mobilnej aplikácii pre platformu iOS a Android.</li> <li>Musí podporovať multi-faktorovú autentifikáciu (MFA) pre zvýšenie bezpečnosti prístupu k zariadeniam a službám</li> <li>PAM server musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu (min. podpora pre VMware ESXi).</li> <li>Musí podporovať externé identity databázy vrátane LDAP databáz.</li> <li>Musí podporovať použitie externých RADIUS serverov.</li> <li>Musí obsahovať intuitívne grafické rozhranie pre IPv4 klientov.</li> <li>Musí mať integrované: <ul style="list-style-type: none"> <li>Monitorovacie schopnosti: <ul style="list-style-type: none"> <li>Systém musí umožňovať nepretržité sledovanie výkonu, stavu a bezpečnosti všetkých komponentov.</li> <li>Musí poskytovať prehľadné a detailné metriky o využití systémových zdrojov, ako sú CPU, pamäť, sieťová priepustnosť a diskové operácie.</li> <li>Musí obsahovať funkcie na detekciu anomálií a generovanie upozornení pri zistení neštandardného správania alebo potenciálnych problémov.</li> </ul> </li> <li>Reportovacie schopnosti:</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>Licencia podporuje 50 až 99 používateľov.</li> <li>FortiPAM integruje FortiToken, ktorý umožňuje MFA prostredníctvom mobilných aplikácií dostupných pre iOS aj Android.</li> <li>FortiPAM podporuje MFA cez SAML, RADIUS a LDAP, čím zabezpečuje bezpečný prístup k zariadeniam a službám.</li> <li>FortiPAM je distribuovaný ako virtuálne zariadenie, ktoré podporuje VMware ESXi.</li> <li>FortiPAM podporuje externé integrácie s LDAP servermi pre autentifikáciu a správu používateľov.</li> <li>FortiPAM umožňuje integráciu s externými RADIUS servermi.</li> <li>FortiPAM poskytuje moderné webové GUI, ktoré podporuje IPv4.</li> <li>FortiPAM umožňuje nepretržité sledovanie výkonu, stavu a bezpečnosti komponentov a obsahuje detekciu anomálií s upozorneniami.</li> <li>FortiPAM poskytuje prehľadné a detailné metriky o využití systémových zdrojov, ako sú CPU, pamäť, sieťová priepustnosť a diskové operácie.</li> <li>FortiPAM obsahuje analyzátor udalostí a systém varovaní, ktorý deteguje anomálie.</li> <li>FortiPAM umožňuje vytvárať a exportovať reporty do PDF.</li> <li>FortiPAM obsahuje pokročilú diagnostiku logov a analýzu udalostí.</li> <li>FortiPAM umožňuje vzdialenú diagnostiku a správu, vrátane integrácie s nástrojmi na správu a údržbu.</li> <li>FortiPAM umožňuje nahrávanie vzdialených relácií vrátane obrazu, zvuku a interakcií.</li> </ul> |

|                         |  |   |
|-------------------------|--|---|
|                         | <ul style="list-style-type: none"> <li>▪ Musí poskytovať možnosť vytvárať prispôsobené reporty podľa potrieb užívateľa, vrátane exportu dát do formátu PDF.</li> <li>○ Diagnostické schopnosti: <ul style="list-style-type: none"> <li>▪ Systém musí obsahovať nástroje na hlbokú diagnostiku problémov, vrátane analýzy logov, sledovania udalostí a trasovania chýb.</li> <li>▪ Musí poskytovať možnosti pre vzdialenú diagnostiku a riešenie problémov, vrátane integrácie s nástrojmi na správu a údržbu.</li> </ul> </li> </ul> <p>Musí podporovať monitorovanie a nahrávanie vzdialených relácií do video formátu.</p> <ul style="list-style-type: none"> <li>• Systém musí umožňovať nahrávanie všetkých aktivít v rámci vzdialených relácií, vrátane obrazovky, zvuku a interakcií používateľa.</li> <li>• Nahrávanie musí byť spúšťané automaticky pri začatí relácie alebo manuálne administrátorom.</li> <li>• Musí podporovať ukladanie nahrávok v bežných video formátoch (napr. WebM) pre jednoduché prehranie a archiváciu.</li> <li>• Systém musí zabezpečiť, že všetky nahrávky a monitorované dáta sú chránené pomocou šifrovania počas prenosu aj pri uložení.</li> <li>• Musí obsahovať mechanizmy na zabezpečenie prístupu k nahrávkam, vrátane autentifikácie a kontroly prístupu.</li> <li>• Systém musí umožňovať centralizované ukladanie nahrávok na bezpečnom úložisku s možnosťou jednoduchej správy, vyhľadávania a prehrávania nahrávok.</li> <li>• Musí podporovať funkcie na archiváciu a dlhodobé uchovávanie nahrávok podľa nastavených politík organizácie.</li> <li>• Systém musí umožňovať generovanie auditných záznamov o všetkých nahratých reláciách, vrátane informácií o čase, trvaní, účastníkoch a iné.</li> <li>• Musí poskytovať nástroje na vytváranie reportov o nahratých a monitorovaných reláciách pre účely auditu a kontroly zhody.</li> <li>• Systém musí mať intuitívne rozhranie, ktoré umožní jednoduché nastavenie, spúšťanie a správu nahrávania a monitorovania relácií.</li> <li>• Musí poskytovať možnosť notifikácií a upozornení pre administrátorov o začiatku, ukončení a výnimočných udalostiach počas relácie.</li> <li>• Systém musí byť kompatibilný s existujúcimi nástrojmi a infraštruktúrou na správu vzdialených relácií.</li> <li>• Musí umožňovať integráciu s inými bezpečnostnými a monitorovacími nástrojmi prostredníctvom štandardných API a protokolov.</li> </ul> | <ul style="list-style-type: none"> <li>• FortiPAM umožňuje pri začatí relácie automatické aj manuálne nahrávanie.</li> <li>• FortiPAM podporuje bežné video formáty ako WebM pre jednoduché prehranie a archiváciu.</li> <li>• FortiPAM využíva šifrovanie pre uložené aj prenášané údaje, monitorované dáta sú chránené pomocou šifrovania počas prenosu aj pri uložení.</li> <li>• FortiPAM poskytuje mechanizmy na zabezpečenie prístupu k nahrávkam prostredníctvom autentifikácie a kontroly prístupu, čím zaisťuje, že len oprávnení používatelia môžu pristupovať k citlivým informáciám.</li> <li>• FortiPAM umožňuje centralizované ukladanie a správu nahrávok na bezpečnom úložisku s možnosťou jednoduchej správy, vyhľadávania a prehrávania nahrávok.</li> <li>• FortiPAM podporuje funkcie na archiváciu a dlhodobé uchovávanie nahrávok v súlade s politikami organizácie.</li> <li>• FortiPAM umožňuje generovanie podrobných auditných záznamov o všetkých nahratých reláciách, vrátane informácií o čase, trvaní a účastníkoch.</li> <li>• FortiPAM poskytuje nástroje na vytváranie reportov o nahratých a monitorovaných reláciách, vrátane informácií o čase, trvaní, účastníkoch a iné čo je užitočné pre audit a kontrolu zhody.</li> <li>• FortiPAM disponuje intuitívnym rozhraním, ktoré umožňuje jednoduché nastavenie, spúšťanie a správu nahrávania a monitorovania relácií.</li> <li>• FortiPAM poskytuje možnosť notifikácií a upozornení pre administrátorov o začiatku, ukončení a výnimočných udalostiach počas relácie. Administrátori môžu monitorovať aktívne relácie v reálnom čase a podľa potreby ich ukončiť.</li> <li>• FortiPAM je navrhnutý tak, aby bol kompatibilný s existujúcimi nástrojmi a infraštruktúrou na správu vzdialených relácií. Podporuje rôzne protokoly a štandardy, čo umožňuje jeho integráciu do rôznych prostredí.</li> <li>• FortiPAM podporuje integráciu s inými bezpečnostnými a monitorovacími nástrojmi prostredníctvom štandardných API a protokolov. Poskytuje REST API, ktoré umožňuje integráciu s rôznymi systémami na správu a monitorovanie.</li> </ul> |
| Rozšírená funkcionality | <ul style="list-style-type: none"> <li>• Musí podporovať spúšťanie min. týchto aplikácií: Putty, Windows Remote Desktop, VNC Viewer, Tight VNC, WinSCP a custom aplikácií.</li> <li>• Podpora TPM pre ochranu privátnych kľúčov.</li> <li>• Podpora DLP na základy typu súboru, veľkosti alebo vodoznaku.</li> <li>• Podpora blokovania príkazov v SSH profile.</li> <li>• Podpora blokovanie clipboardu v RDP.</li> </ul>   | <ul style="list-style-type: none"> <li>• FortiPAM podporuje spúšťanie aplikácií ako PuTTY, Windows Remote Desktop, VNC Viewer, Tight VNC, WinSCP a custom aplikácií.</li> <li>• FortiPAM podporuje TPM pre ochranu privátnych kľúčov</li> <li>• FortiPAM podporuje DLP na základy typu súboru, veľkosti alebo vodoznaku.</li> <li>• FortiPAM podporuje blokovanie príkazov v SSH profile.</li> </ul>  |



|                     |  |   |
|---------------------|--|---|
|                     | <ul style="list-style-type: none"> <li>• Podpora pre Approve menežmentu (schvaľovanie požiadaviek na prístup).</li> <li>• Podpora autoamatickej zmeny hesla.</li> <li>• Podpora anti-virusového skenovania pre prenos súborov cez web rozhranie.</li> </ul>                  | <ul style="list-style-type: none"> <li>• FortiPAM podporuje blokovanie clipboardu v RDP.</li> <li>• FortiPAM podporuje Approve menežment (schvaľovanie požiadaviek na prístup).</li> <li>• FortiPAM podporuje automatickú zmenu hesla.</li> <li>• FortiPAM podporuje anti-virusové skenovanie pre prenos súborov cez web rozhranie.</li> </ul>  |
| Manažment platforma | Podpora viacerých správco a rôznych úrovni prístupových oprávnení.<br>Podpora odosielania logov na SYSLOG server.  | FortiPAM poskytuje kontrolu prístupu k privilegovaným účtom, kde používatelia môžu pristupovať k zdrojom FortiPAM na základe svojich rolí, ako sú štandardný používateľ alebo administrátor.<br><br>FortiPAM podporuje odosielanie logov na FortiAnalyzer prostredníctvom protokolu Syslog na porte TCP/514.  |
| Podpora od výrobcu  | Min. na 3 roky v režime 8x5xNBD.   | Pre uvedený FortiPAM bude zabezpečená podpora od výrobcu na 3 roky v režime 8x5xNBD.  |
| Inštalácia          | súčasťou ponuky musí byť inštalačná služba obsahujúca dodávku, inštaláciu a nastavenie dodaných softvérov, odskúšanie funkčnosti a prevádzkyschopnosti, uvedenie do prevádzky, zaškolenie kupujúcim určených osôb, vrátane inštalácie všetkých súčastí operačných prostredí. | Súčasťou ponuky je komplexná inštalačná služba, ktorá zahŕňa zabezpečenie dodávky, dopravy, odbornú inštaláciu a konfiguráciu dodaných softvérov. Táto služba zahŕňa aj testovanie funkčnosti a overenie prevádzkovej spoľahlivosti, uvedenie do plnej prevádzky a poskytnutie školenia pre určené osoby kupujúceho, vrátane nasadenia všetkých potrebných súčastí operačných systémov. |

## 6. Centrálna autentizácia, autorizácia a účtovanie (AAA) + systém viacfaktorovej autentizácie (MFA)

Tabuľka č. 6

| Parameter:             | Minimálne požadované parametre:   | Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru  |
|------------------------|---|---|
|                        | <p>Centrálna autentizácia, autorizácia a účtovanie (AAA) zabezpečuje komplexné riadenie prístupu používateľov k sieťovým zdrojom a službám v rámci organizácie. Súčasťou riešenia je aj viacfaktorová autentizácia (MFA), ktorá pridáva ďalšiu vrstvu ochrany prístupu tým, že vyžaduje overenie identity používateľa pomocou viacerých nezávislých autentifikačných faktorov, ako sú jednorazové heslá (OTP).</p> <p><i>Je nutné uviesť detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (Part Number, Product Code)</i></p> | <p>Centrálna autentizácia, autorizácia a účtovanie (AAA) + systém viacfaktorovej autentizácie (MFA) od výrobcu Fortinet, Inc. s Product Code: FAC-VM-Base a FTM-ELIC-50, ktorá bude obsahovať uvedenú detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (product code):</p> <p>5x FAC-VM-Base (FortiAuthenticator)<br/> 15x FC1-10-0ACVM-248-02-12 (rozšírenie počtu podporovaných používateľov)<br/> 1x FTM-ELIC-50 (FortiToken Mobile)</p> <p><a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf</a></p> <p><a href="https://docs.fortinet.com/document/fortiauthenticator/6.6.2/administration-guide/873492">https://docs.fortinet.com/document/fortiauthenticator/6.6.2/administration-guide/873492</a></p> <p><a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf</a></p> <p><a href="https://docs.fortinet.com/document/fortitoken/latest/comprehensive-guide/718181/introduction">https://docs.fortinet.com/document/fortitoken/latest/comprehensive-guide/718181/introduction</a></p> |
| Počet:                 | 5 ks, ktorý musí byť dodaný vo forme virtuálneho zariadenia pre virtualizačnú platformu.  | v počte 5ks bude vo forme virtuálneho zariadenia pre virtualizačnú platformu  |
| Vysoká dostupnosť      | Podpora vysokej dostupnosti v konfigurácii Active-Passive, alebo Active-Active.   | <p>FortiAuthenticator podporuje vysokú dostupnosť (HA) v dvoch režimoch:</p> <ul style="list-style-type: none"> <li>Cluster (Active-Passive): V tomto režime je jedna jednotka aktívna a druhá v pohotovostnom režime. V prípade zlyhania aktívnej jednotky preberá pohotovostná jednotka jej úlohy. Všetky nastavenia sú medzi týmito zariadeniami synchronizované.</li> <li>Load-Balancing (Active-Active): Tento režim umožňuje, aby jedna jednotka fungovala ako primárna a až desať ďalších jednotiek ako load-balancery. Zátťaž môže byť rozdelená medzi zariadenia pomocou round-robin DNS, distribúcie záťaže klientov autentifikácie (Auth/NAS) alebo externých zariadení na vyvažovanie záťaže. Tento režim je určený predovšetkým pre nasadenia dvojfaktorovej autentifikácie, pričom sa synchronizuje len podmnožina konfigurácie medzi zariadeniami.</li> </ul>  |
| Základná funkcionality | <ul style="list-style-type: none"> <li>Musí podporovať správu minimálne 100 zariadení.</li> <li>Musí poskytovať flexibilné a granulórne spravovanie IPv4 sietí s podporou auditovania a reportovania.</li> <li>musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu, min. s podporou VMware ESXi</li> </ul>   | <ul style="list-style-type: none"> <li>Každá základná licencia FortiAuthenticator-VM (FAC-VM-Base) podporuje až 100 používateľov. Počet podporovaných zariadení (napr. autentifikačných klientov) je odvodený od počtu používateľov.</li> <li>FortiAuthenticator poskytuje centralizovanú správu autentifikácie a autorizácie, vrátane podpory RADIUS a TACACS+ protokolov, čo umožňuje granulórne riadenie prístupu v IPv4 sieťach. Systém tiež ponúka rozsiahle možnosti auditovania a reportovania pre sledovanie autentifikačných udalostí.</li> <li>FortiAuthenticator bude dodaný ako virtuálne zariadenie s podporou</li> </ul>  |

|                         |  |   |
|-------------------------|--|---|
|                         | <ul style="list-style-type: none"> <li>Musí poskytovať flexibilný nástroj na vytváranie modelu politík na základe pravidiel a atribút, tak aby bolo možné pokryť aj zložité a komplexné požiadavky na policy model.</li> <li>Musí obsahovať intuitívne grafické rozhranie pre IPv4 klientov.</li> <li>Musí mať integrované monitorovacie, reportovacie aj diagnostické schopnosti pre maximálnu kontrolu a visibilitu.</li> <li>Musí podporovať externé identity databázy vrátane min. Windows Active Directory, LDAP databáz.</li> <li>Musí podporovať použitie externých RADIUS serverov.</li> <li>Systém musí poskytovať mobilnú aplikáciu dostupnú pre zariadenia so systémami iOS (Apple App Store) a Android (Google Play Store).</li> <li>Aplikácia musí umožňovať prijímanie push notifikácií ako druhý faktor autentifikácie.</li> <li>Systém musí umožňovať zasielanie push notifikácií na mobilné zariadenia používateľov pre potvrdenie autentifikácie.</li> <li>Push notifikácie musia obsahovať informácie o prihlasovacej relácii (napr. čas, miesto, zariadenie), aby používateľ mohol overiť legitímnosť požiadavky.</li> <li>Systém musí byť schopný podporovať minimálne 50 používateľov s možnosťou škálovania na vyšší počet podľa potrieb organizácie.</li> <li>Mobilná aplikácia a systém pre MFA musia zabezpečiť šifrovaný prenos dát medzi zariadením používateľa a autentifikačným serverom.</li> </ul> <p>Systém musí podporovať silné bezpečnostné mechanizmy na ochranu údajov používateľov, vrátane ochrany proti phishingu a iným formám útokov.</p> | <p>viacerých virtualizačných platforiem, vrátane VMware ESXi.</p> <ul style="list-style-type: none"> <li>FortiAuthenticator umožňuje vytváranie komplexných autentifikačných a autorizačných politík na základe rôznych pravidiel a atribútov, čo umožňuje prispôbenie sa špecifickým potrebám organizácie.</li> <li>FortiAuthenticator disponuje intuitívnym webovým grafickým rozhraním, ktoré umožňuje jednoduchú správu a konfiguráciu pre IPv4 klientov a administrátorov.</li> <li>FortiAuthenticator poskytuje integrované nástroje na monitorovanie, reportovanie a diagnostiku autentifikačných procesov, čo zabezpečuje maximálnu kontrolu a prehľad o stave systému.</li> <li>FortiAuthenticator podporuje integráciu s externými identitnými databázami, vrátane Windows Active Directory a LDAP, čo umožňuje centralizovanú správu používateľov.</li> <li>FortiAuthenticator môže fungovať ako RADIUS server a zároveň podporuje integráciu s externými RADIUS servermi pre autentifikáciu a autorizáciu.</li> <li>FortiAuthenticator v kombinácii s FortiToken Mobile poskytuje mobilnú aplikáciu dostupnú pre iOS a Android zariadenia, ktorá slúži na generovanie jednorazových hesiel (OTP) pre dvojfaktorovú autentifikáciu.</li> <li>FortiToken Mobile podporuje prijímanie push notifikácií pre dvojfaktorovú autentifikáciu, čo zjednodušuje proces overovania pre používateľov.</li> <li>FortiAuthenticator v spolupráci s FortiToken Mobile umožňuje zasielanie push notifikácií na mobilné zariadenia používateľov pre potvrdenie autentifikácie.</li> <li>FortiToken Mobile push notifikácie obsahujú informácie o prihlasovacej relácii, čo umožňuje používateľom overiť legitímnosť autentifikačnej požiadavky.</li> </ul> |
| Rozšírená funkcionality | <ul style="list-style-type: none"> <li>Musí podporovať použitie automatického enrollmentu certifikátov pre štandardné PC aj mobilné platformy.</li> <li>Musí mať možnosť spravovať svoje zariadenia cez self-service portál a bude podporovať SAML 2.0 pre webové portály.</li> <li>Musí podporovať platformy Android a iOS.</li> <li>Musí poskytovať možnosť správy a bezpečného doručovania certifikátov pre účely vytvárania IPsec VPN autentizovaných pomocou certifikátov.</li> <li>Musí podporovať 802.1x autentizáciu.</li> </ul> <p>Musí mať možnosť obsluhovať min. 100 používateľov.</p>   | <ul style="list-style-type: none"> <li>FortiAuthenticator podporuje automatický zápis certifikátov prostredníctvom protokolu SCEP (Simple Certificate Enrollment Protocol), čo umožňuje automatizovaný zápis certifikátov pre rôzne zariadenia vrátane štandardných PC a mobilných platforiem.</li> <li>FortiAuthenticator poskytuje self-service portál, ktorý umožňuje používateľom spravovať svoje zariadenia, vrátane registrácie zariadení a správy certifikátov. Okrem toho podporuje SAML 2.0 pre integráciu s webovými portálmi, čo umožňuje jednotné prihlásenie (SSO) a centralizovanú autentifikáciu.</li> <li>FortiAuthenticator v kombinácii s FortiToken Mobile poskytuje podporu pre mobilné platformy Android a iOS, čo umožňuje používateľom využívať mobilné aplikácie na dvojfaktorovú autentifikáciu.</li> <li>FortiAuthenticator umožňuje správu a bezpečné doručovanie certifikátov prostredníctvom protokolu SCEP, čo je obzvlášť užitočné pri nasadzovaní IPsec VPN autentizovaných pomocou certifikátov.</li> <li>FortiAuthenticator podporuje 802.1x autentizáciu, čo umožňuje zabezpečený prístup k sieťovým zdrojom prostredníctvom overovania používateľov a zariadení pred pripojením k sieti.</li> <li>FortiAuthenticator-VM (FAC-VM-Base) podporuje min. 100</li> </ul>   |

|                     |  |   |
|---------------------|--|---|
|                     |  | používateľov.   |
| Manažment platforma | Podpora viacerých správcov a rôznych úrovní prístupových oprávnení.<br>Podpora odosielania logov na SYSLOG server.   | <ul style="list-style-type: none"> <li>• FortiAuthenticator umožňuje vytvárať viacerých administrátorských používateľov s rôznymi úrovňami prístupových oprávnení. Administrátori môžu byť priradení k rôznym rolám a skupinám, čo umožňuje detailné riadenie prístupu a povolení v rámci systému. Týmto spôsobom je možné zabezpečiť, že každý správca má prístup len k tým funkciám a údajom, ktoré sú pre jeho úlohu nevyhnutné.</li> <li>• FortiAuthenticator podporuje odosielanie logov na vzdialené SYSLOG servery. Umožňuje konfiguráciu až 20 SYSLOG serverov, na ktoré môže zasielať systémové a debug logy.</li> </ul> |
| Podpora od výrobcu  | Min. na 3 roky v režime 8x5xNBD.   | Pre produkty bude zabezpečená podpora od výrobcu na 3 roky v režime 8x5xNBD.  |
| Inštalácia          | súčasťou ponuky musí byť inštalačná služba obsahujúca dodávku, inštaláciu a nastavenie dodaných softvérov, odskúšanie funkčnosti a prevádzkyschopnosti, uvedenie do prevádzky, zaškolenie kupujúcim určených osôb, vrátane inštalácie všetkých súčastí operačných prostredí. | Súčasťou ponuky je komplexná inštalačná služba, ktorá zahŕňa zabezpečenie dodávky, dopravy, odbornú inštaláciu a konfiguráciu dodaných softvérov. Táto služba zahŕňa aj testovanie funkčnosti a overenie prevádzkovej spoľahlivosti, uvedenie do plnej prevádzky a poskytnutie školenia pre určené osoby kupujúceho, vrátane nasadenia všetkých potrebných súčastí operačných systémov.   |