|  |
| --- |
| **OSNOVNI ZAHTJEVI TEHNIČKE FUNKCIONALNOSTI** |

Tablice Osnovnih tehničko-funkcionalnih zahtjeva navedene u sljedećim paragrafima moraju sadržavati DA/NE odgovore na opis tehničke karakteristike i broj stranice Ponude gdje je priložena TEHNIČKA DOKUMENTACIJA PROIZVOĐAČA I/ILI POTVRDA PROIZVOĐAČA ili jednakovrijedan dokument kojim dokazuje sljedeće TEHNIČKO FUNKCIONALNE KARAKTERISTIKE ponuđenog proizvoda.

Tablice tehničko-funkcionalnih zahtjeva navedene u sljedećim paragrafima moraju sadržavati DA/NE odgovore na opis tehničke karakteristike, te ih je ispunjene ponuditelj obvezan priložiti u ponudi. Obveza je Ponuditelja izrijekom navesti točnu specifikaciju (proizvođač, model, tehničku dokumentaciju proizvođača ponuđenog rješenja, navesti broj stranice ponude gdje se nalazi) svake komponente sustava koja se nalazi u ponudi, a kojom se zadovoljavaju pojedini tehničko-funkcionalni zahtjevi.

Priložene tablice se popunjavaju na način da se:

* u stupac Zadovoljava (DA/NE) upisuje DA za slučaj da ponuđeno podržava određeni zahtjev, ili NE za slučaj da ponuđeno ne podržava određeni zahtjev,
* u stupac Dokaz i veze na priloženu karakteristikuupisuje se naziv i broj stranice dokumenta proizvođača ponuđene opreme priloženog u ponudi kojim se dokazuje određeni zahtjev iz tablice, prevedenog na hrvatski jezik.

Ponuditelj mora dokazati da ponuđeno zadovoljava sve tražene uvjete iz ove Specifikacije zahtjeva.

Ponuditelj mora dostaviti u ponudi gore navedenu tehničku dokumentaciju kojom dokazuje ispunjenje navedenih zahtjeva. U slučaju postojanja sumnje u istinitost podataka navedenih u priloženim dokumentima koje su ponuditelji dostavili, javni naručitelj može radi provjere istinitosti podataka:

* od ponuditelja zatražiti da u primjerenom roku dostave izvornike ili
* ovjerene preslike tih dokumenata i/ili
* obratiti se izdavatelju dokumenta i/ili nadležnim tijelima i/ili
* provjeriti na službenim web stranicama proizvođača.

|  |
| --- |
| * 1. **Sustav za zaštitu prometa elektroničke pošte**
 |
| PONUĐENI PROIZVOĐAČ, MODEL: |
| Ponuditelj u ponudi treba dostaviti proizvođačku deklaraciju ili jednakovrijedan dokument kojim dokazuje sljedeće karakteristike ponuđenog proizvoda |
| Redni broj | Opis tehničke karakteristike | Zadovoljava tražene karakteristike (DA/NE) | Dokaz i veze na priložene dokumente |
| Opće karakteristike sustava |
| 1 | Ugradivo u 19“ ormar. |  |  |
| 2 | Minimalno dva izmjenjiva napajanja (AC) po komponenti sustava. |  |  |
| 3 | Radna temperatura u minimalnom rasponu od +10ºC do +35ºC. |  |  |
| Funkcionalnosti  |
| 4 | Mrežno upravljačko sučelje 1G RJ-45. |  |  |
| 5 | Ukupan broj mrežnih sučelja se mora odabrati na način da se osigura visoka dostupnost i skalabilnost na nivou uređaja, na nivou cijelog sustava i njegovog spoja na mrežnu infrastrukturu naručitelja. Sučelja prema mrežnoj infrastrukturi naručitelja trebaju uključivati primopredajnike i trebaju biti 10G sučelja po 10GBASE-SR standardu te trebaju podržavati 802.1Q. Minimalni broj sučelja prema naručitelju je 2x10G. |  |  |
| 6 | Sustav mora obraditi minimalno 75.800 poruka elektroničke pošte u satu. |  |  |
| 7 | Sustav mora podržavati minimalno 520.000 korisničkih računa (sandučića elek. pošte). |  |  |
| 8 | Sustav mora podržavati konfiguriranje minimalno 2 (slovima: dva) MTA (engl. Mail transfer agent), po jedan za svaki interni MX. |  |  |
| 9 | Podrška za IPv4 i IPv6 za sve navedene funkcionalnosti sigurnosne zaštite. |  |  |
| 10 | Detekcija i blokiranje poruka elektroničke pošte prema:* Malicioznom privitku,
* Tipu privitka (npr. .exe, .dll, .sh, …),
* Malicioznoj poveznici unutar e. poruke,
* Reputaciji i kategorizaciji URL-a unutar e. poruke
* Skraćenoj malicioznoj poveznici unutar e. poruke,
* Naslovu poruke,
* Ključnim riječima unutar tijela poruke.
 |  |  |
| 11 | Mogućnost prepoznavanja zlonamjernih datoteka na osnovi kriptografskog sažetka, potpisa ili drugih definicija. |  |  |
| 12 | Mogućnost provjere sadržaja unutar arhiviranih i komprimiranih datoteka (bez dodatne kriptografske zaštite) za sljedeće formate:- ZIP format,- RAR format,- 7Z format,- gzip format,- ARJ format,- CAB format. |  |  |
| 13 | Mogućnost detekcije i blokiranje masovne kampanje (kampanje usmjerene na veliki broj korisnika). |  |  |
| 14 | Mogućnost spremanja poruka u karantenu:* zadržavanje (pohrana) poruka elektroničke pošte s malicioznim privitkom,
* zadržavanje (pohrana) poruka elektroničke pošte s malicioznom poveznicom,
* zadržavanje (pohrana) poruka elektroničke pošte blokiranih prema drugim uvjetima,
* mogućnost jednostavnog otpuštanja poruka elektroničke pošte iz karantene od strane administratora i primatelja poruke elektroničke pošte ,
* automatsko brisanje poruka elektroničke pošte iz karantene starijih od vremenskog perioda definiranog od strane administratora.
 |  |  |
| 15 | Prepoznavanje i blokiranje poruka elekt. pošte:• Prepoznavanje i blokiranje ulaznih poruka elekt. pošte pristiglih iz nepouzdanih izvora • Blokiranje ulaznih poruka prema zadanom/odabranom tipu (ekstenziji) datoteke • Prepoznavanje i blokiranje izlaznih poruka elekt. pošte s nedopuštenim sadržajem |  |  |
| 16 | Kreiranje vlastitih crnih lista i lista izuzimanja („black and white lists“):* mogućnost kreiranja listi prema odredišnoj adresi,
* mogućnost kreiranja listi prema izvorišnoj adresi,
* mogućnost kreiranja listi prema naslovu poruke,
* mogućnost kreiranja listi prema ključnim riječima.
 |  |  |
| 17 | Redovno ažurirane i aktualne baze:* zlonamjernih domena,
* zlonamjernih URL-ova,
* zlonamjernih IP adresa i adresnih raspona,
* potpisa i/ili kriptografskih sažetaka zlonamjernih datoteka,
* zlonamjernih pošiljatelja (nepouzdani izvori).
 |  |  |
| 18 | Obavještavanje:* mogućnost slanja obavijesti administratoru sustava o zlonamjernim aktivnostima,
* mogućnost slanja obavijesti primatelju poruke kojem je upućena maliciozna poruka (poruka sa malicioznim URL-om ili privitkom),
* mogućnost upravljanja slanja obavijesti primatelju poruke ovisno o tipu/mehanizmu detekcije zlonamjerne poruke,
* mogućnost prilagodbe forme i sadržaja poruka koje se šalju prema primateljima poruka.
 |  |  |
| 19 | Blokiranje neželjene pošte („antispam“):* mogućnost blokiranja neželjene pošte,
* mogućnost blokiranja masovnih reklamnih poruka.
 |  |  |
| 20 | Mogućnost slanja dnevničkih zapisa (eng.*log)* u *syslog* formatu uz zadržavanje lokalnih dnevničkih zapisa. |  |  |
| 21 | Upravljanje:* ugrađena podrška za pristup i administraciju uređaja putem grafičkog sučelja za kontrolu uređaja (GUI),
* mogućnost konfiguracije uređaja direktnim spajanjem putem CLI/komandne linije,
* mogućnost redovnog centraliziranog ažuriranja softvera i sigurnosnih definicija,
* ugrađena mogućnost upravljanja, izvoza i uvoza prijašnjih konfiguracija.
 |  |  |
| 22 | Sigurnosni sustav za zaštitu mora podržavati konfiguraciju visoke dostupnosti (redundancija komponenti na lokaciji) rada svih komponenti sustava u slučaju kvarova, ispada i prekida rada. |  |  |
| 23 | Mogućnost izvještavanja na više načina:* prikaz statistike o ukupnom broju obrađenih poruka elekt. pošte,
* prikaz statistike prema načinu detekcije (maliciozna poveznica/privitak itd.),
* prikaz statistike prema pošiljatelju i primatelju elekt. pošte po broju poslanih i primljenih poruka elekt. pošte
* prikaz statistike top poruka elekt. pošte prema izvorišnom/destinacijskom poslužitelju
* statistički prikaz gore opisanog prema zadanom vremenskom razdoblju,
* mora podržavati isporuku izvještaja u jednom od sljedećih formata: PDF, HTML, CSV, DOC, DOCX .
 |  |  |
| 24 | Licence za sve gore navedene funkcionalnosti u trajanju od 5 (slovima: pet) godina |  |  |
| 25 | Sustav omogućuje analizu datoteka u izoliranom okruženju (eng. *sandboxing*) od minimalno 1.000 jedinstvenih datoteka u satu. |  |  |
| 26 | Uređaj treba moći propusti transparentno sve što prelazi tražene kapacitete inspekcije bez odbacivanja prometa do maksimalne tražene mrežne propusnosti. |  |  |