|  |
| --- |
| **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 Internet prometa svih škola**
 |
| 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 | Sve komponente su ugradive u 19“ ormar. |  |  |
| 2 | Minimalno dva izmjenjiva napajanja (AC) po komponenti sustava. |  |  |
| 3 | Radna temperatura u minimalnom rasponu od +10ºC do +35ºC. |  |  |
| 4 | Fizička veličina sustava je jednaka ili manja od 22 RU (Rack Unit). |  |  |
| Funkcionalnosti  |
| 5 | Mrežno upravljačko sučelje 1G RJ-45. |  |  |
| 6 | Ukupan broj sučelja čini broj sučelja kojim se spaja na Naručiteljevu infrastrukturu, sučelja koja se koriste za interna spajanja unutar sustava (ovise o rješenju i naručitelj ne može znati broj) te broj sučelja koji zadovoljavaju uvijete skalabilnosti i visoke dostupnosti. Spoj sustava na mrežu Naručitelja mora se moći izvesti minimalno sa uključenim sučeljima i primopredajnicima prema slijedećim karakteristikama : * 16 x 10G sučelja po 10GBASE-SR standardu. 8x10G za svaku granu (A i B). Sučelja 10G će se koristiti za spajanje kod implementacije,
* 4 x 100G sučelja po 100GBASE-SR4 standardu. 2x100G za svaku granu (A i B) Sučelja 100G će se koristiti u budućnosti.
* Protokol 802.3ad (LACP) - grupiranje do 8 10G sučelja i grupiranje do 2 100G sučelja
* 9100 MTU
* 802.1Q (VLAN tagging)
* Full-duplex
 |  |  |
| 7 | Minimalna propusnost uređaja od 100 Gbps. Specifikacija propusnosti prema stavkama ispod. Sve stavke podrazumijevaju zbroj ukupne propusnosti. Propusnosti se odnose na prosječnu veličinu paketa od 950 Byta.* 80 Gbps – minimalna mrežna propusnost sustava klasičnog usmjeravanja i inspektiranja paketa na 2 i 3 razini TCP/IP modela (stateful FW) tj bez uključenih naprednih inspekcija na višim razinama modela,
* 16 Gbps – minimalna propusnost sustava sa svim uključenim traženim sigurnosnim funkcionalnostima i sustavima napredne zaštite,
* 4 Gbps – minimalna propusnost sustava sa TLS/SSL dekripcijom i sa svim uključenim traženim sigurnosnim funkcionalnostima i sustavima napredne zaštite.
 |  |  |
| 8 | Minimalni broj istovremenih sesija – 10.000.000 |  |  |
| 9 | Minimalni broj novih sesija (novih sesija po sekundi) - 200.000 |  |  |
| 10 | Podrška za IPv4 i IPv6 za sve navedene funkcionalnosti sigurnosne zaštite. |  |  |
| 11 | Mogućnost provjere datoteka prenesenih preko mreže putem nesigurnih tj. ne kriptiranih/ne šifriranih protokola. |  |  |
| 12 | Mogućnost prepoznavanja zlonamjernih datoteka na osnovi kriptografskog sažetka, potpisa ili drugih definicija. |  |  |
| 13 | Mogućnost filtriranja DNS prometa:* blokiranje
* *sinkholing*
 |  |  |
| 14 | Mogućnost otkrivanja i prevencije zlonamjernih mrežnih aktivnosti – IPS  |  |  |
| 15 | Mogućnost provjere sadržaja unutar arhiviranih i kompromitiranih datoteka (bez dodatne kriptografske zaštite) za sljedeće formate:* ZIP format,
* RAR format,
* 7Z format,
* gzip format,
* ARJ format,
* CAB format.
 |  |  |
| 16 | Mogućnost prepoznavanja i blokiranja potencijalno zlonamjernog prometa sa/prema IP adresama i adresnim prostorima s lošom reputacijom za:* skeniranja,
* pokušaje iskorištavanja ranjivosti,
* pokušaje neovlaštenog pristupa,
* komunikacija s C&C poslužiteljima.
 |  |  |
| 17 | Mogućnost dekripcije TLS/SSL prometa. Za potrebe dekripcije TLS 1.3 protokola dopuštena je degradacija na isključivo TLS 1.2 protokol |  |  |
| 18 | TLS/SSL inspekcija s terminacijom TLS /SSL veza na sigurnosnom sustavu u svrhu provođenja analize nad dekriptiranim/ dešifriranim prometom uz uspostavljanje nove TLS/SSL veze između sigurnosnog sustava i krajnjeg uređaja korištenjem svojih certifikata. |  |  |
| 19 | Mogućnost isključivanja forsiranog TLS/SSL degradiranja kod dekripcije/ dešifriranja u svrhu povećanja performansi rješenja. |  |  |
| 20 | Mogućnost kreiranja politika za TLS/SSL dekripciju uz mogućnost kreiranja iznimki tj izuzimanja za TLS/SSL dekripciju na temelju izvorišnih i odredišnih IP adresa, odredišnih kategorija i pojedinačnih razlikovnih imena (DN - distinguished name). |  |  |
| 21 | Redovno ažurirane i aktualne baze:* zlonamjernih domena,
* zlonamjernih URL-ova,
* zlonamjernih IP adresa i adresnih raspona,
* potpisa i/ili kriptografskih sažetaka zlonamjernih datoteka,
* IPS/IDS potpisa/pravila,
* poznatih servisa koji iz tehničkih razloga ne podržavaju TLS/SSL dekripciju.
 |  |  |
| 22 | Redovno ažurirana i aktualna baza poznatih servisa za potrebu izuzimanja (eng. *whitelisting*) istih iz inspekcije. Identificirani servisi trebaju imati visok stupanj razlučivosti tj unutar jednog davatelja usluga identificirati različite usluge/servise. Ažurirani popisi se moraju jednostavno i automatski ažurirati i primijeniti na mehanizam izuzimanja. |  |  |
| 23 | Dokumentirana IPS/IDS pravila uz dodatne opise prijetnji, zahvaćenih uređaja/programa, ozbiljnosti i prirode napada (CVSS), posljedice i pripadajuće CVE oznake. |  |  |
| 24 | Mogućnost slanja dnevničkih zapisa (eng.*log)* u *syslog* formatu uz zadržavanje lokalnih dnevničkih zapisa. |  |  |
| 25 | Podrška za upravljanje i konfiguriranje uređaja putem REST API-a za slijedeće:* kreiranje i upravljanje mrežnim objektima (IP adresama, IP adresnim rasponima te skupovima i kombinacijama istih),
* kreiranje pravila za izuzimanje (eng. *whitelisting*) i upravljanje istima,
* kreiranje pravila vatrozida i upravljanje istim pravilima,
* kreiranje sigurnosnih profila i upravljanje istima,
* upravljanje konfiguracijom mrežnih sučelja,
* upravljanje tablicama usmjeravanja.
 |  |  |
| 26 | Idejno rješenje mora biti osmišljeno na način da omogućava skalabilnost, tj. mogućnost povećanja propusnosti minimalno dvostruko tj 100% u odnosu na trenutno raspisane kapacitete i propusnosti. |  |  |
| 27 | Sigurnosni sustav za zaštitu mora podržavati konfiguraciju visoke dostupnosti (redundancija komponenti) rada svih komponenti sustava u slučaju kvarova, ispada i prekida rada pojedine fizičke, funkcionalne ili logičke cjeline. |  |  |
| 28 | Mogućnost izvještavanja na više načina:* statistički prikaz detektiranih zlonamjernih pojava zadanoj štićenoj IP adresi/domeni ili rasponu IP adresa,
* statistički prikaz svih detektiranih zlonamjernih pojava po broju detektiranih/blokiranih,
* statistički prikaz jedne zadane detektirane zlonamjerne pojave po broju ukupno detektiranih/blokiranih,
* statistički prikaz gore opisanog prema zadanom vremenskom razdoblju,
* mora podržavati isporuku izvještaja u jednom od sljedećih formata: PDF, HTML, CSV, DOC, DOCX.
 |  |  |
| 29 | Potrebne licence za sve gore navedene funkcionalnosti u trajanju od minimalno 5 (slovima: pet) godina . |  |  |
| 30 | Svi elementi u sustavu moraju podržavati upravljačko nadzorne protokole:* SNMPv2, SNMPv3,
* SSHv2,
* Syslog,
* NTP,
* AAA putem RADIUS protokola
 |  |  |
| 31 | Podrška za jedan od slijedećih dinamičkih usmjerivačkih (ruting) protokola: OSPFv2, OSPFv3 ili BGP. Podrška za 20 000 ruta. |  |  |
| 32 | Podrška za propagaciju ruta na dva načina/moda:Mod usmjeravanja („*routing*“ mod)Transparentni mod |  |  |
| 33 | Uređaji sa spajanje sustava na mrežnu infrastrukturu Naručitelja moraju imati uključenu tehnologiju za L3/L4 balansiranje/uravnoteženje prometa sa slijedećim značajkama:* Usmjeravanje prometa na ulaznom sučelju prema L3/L4 značajkama, a neovisno o L2/L3 usmjerivačkim tablicama
* Balansiranje opterećenja temeljeno na težini/vrijednosti čvora
* L4 balansiranje opterećenja temeljeno na virtualnom IP-u
* Balans opterećenja na velikom broju uređaja/poslužitelja
* Podržana visoka dostupnost (eng *failover*) u slučaju ispada čvora
* Funkcionalnost provjere dostupnosti udaljenog IP uređaja putem ICMP proba a u svrhu manipuliranja usmjeravanja prometa
* N + M redundancija (N broj čvorova i M broj hot-standby-eva)
* Automatska reakcija u slučaju kvarova poslužitelja/uređaja
* Usklađena dvosmjernost tokova. Promet iz A–>B i B–>A ide na isti čvor
* Mogućnost preusmjeravanja prometa linearnom brzinom na sve uređaje
* Sposobnost stvaranja klastera uređaja jednog servisa neovisnih o generaciji, modelu ili proizvođaču uređaja
* Ljepljive sesije tj. perzistentne sesije na temelju IP adrese (IP-stickiness)
* VRF podrška,
* Funkcionalnost udruživanja fizickih linkova na dva razlicita uredaja u jednu logicku vezu (virtual Link Aggregation)
* Podržavati IPv4 i IPv6
 |  |  |