# V. TEHNIČNA SPECIFIKACIJA

Ponudnik mora za ponujeno rešitev podati tehnične podatke za opremo, ki je ponujena. Iz tehničnih podatkov mora biti jasno razvidno ali ponujena oprema ustreza tehničnim zahtevam naročnika. Če ponujena oprema ne ustreza tehničnim zahtevam, bo naročnik tako ponudbo označil za nedopustno.

**2 kosa – Požarna pregrada nove generacije za centralno lokacijo**

**Ponujeno:**

**Model \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Proizvajalec \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Oprema mora vključevati garancijo proizvajalca za čas trajanja pogodbe (tovarniška podpora za nadgradnjo in odpravo napak na strojni in programski opremi) za vso ponujeno strojno in programsko opremo.

**Minimalne zahtevane lastnosti strojne opreme za požarno pregrado (za posamezno napravo).**

* Velikost strojne opreme ne več kot 1 RU z možnostjo vgradnje v obstoječo komunikacijsko omaro
* 1x CPU, 4x physical cores
* Vsaj 16 ali več GB RAM
* Vsaj 240GB SSD storage
* Priključna vrata
  1. Najmanj 8x 10/100/1000Base-T RJ45 priključki
  2. Najmanj 4x 1000Base-F SFP priključki (brez transceiverjev)
  3. Ločena vrata za povezavo HA in upravljanje
  4. Možnost delovanja vrat v različnih načinih (trust, untrust, DMZ,…)
* Redundantni napajalnik (N+1) 220 V AC
* Delovanje naprave v temperaturnem razponu od 0 do 40°C
* Skladnost z okoljskimi standardi kot so npr. ROHS II, ISO14001
* Garancija proizvajalca: 3 leta, garantiran čas odprave strojne napake NBD

**Performančne zahteve požarne pregrade:**

* Prepustnost požarne pregrade vsaj 1,5 Gbps realnega prometa (tipična Internetna protokolna distribucija, paketi z L3/L4 vsebino, ter tipična distribucija velikost paketov – npr. IMIX) z vključenimi zahtevanimi varnostnimi mehanizmi.
* Prepustnost požarne pregrade vsaj 500Mbps realnega prometa (tipična Internetna protokolna distribucija, paketi z L7 vsebino, ter tipična distribucija velikost paketov – npr. IMIX) z vključenimi zahtevanimi varnostnimi mehanizmi ter dekripcijo HTTPS (razmerje dekriptiranega HTTPS/ostalo = 40/60%).
* Število hkratnih sej preko požarne pregrade vsaj 2.800.000.
* Število novih sej na sekundo vsaj 120.000.

**Minimalne zahtevane lastnosti programske opreme – požarna pregrada:**

* Podpora agregaciji mrežnih povezav 802.3ad.
* Delovanje v L3 načinu (routing mode).
* Podpora za first hop redundancy protokol (VIP naslov za kliente).
* Podpora združevanju dveh ali več požarnih pregrad v gručo (cluster) na način Active-Active in Active-Passive.
* Sinhronizacija sej med člani gruče.
* »Stateful« požarna pregrada.
* Podpora mehanizmom za usmerjanje:
  + Statične route
  + Multicast route
  + OSPFv2 in v3
  + BGP
  + RIP
  + PIM-SM, PIM-SSM, PIM-DM
  + IGMP v2 in v3
* Podpora za IPv6 protokol:
  + Podpora funkcionalnostim: požarna pregrade, varnostno pregledovanje prometa (npr. URL filtering, IPS, blokiranje aplikacij)
  + Identifikacija uporabnikov
  + NAT66 in NAT64
* Integracija z aktivnim imenikom.
* Podpora centralnemu upravljanju in nadzoru
* Podpora centralnemu logiranju

**Zahtevani varnostni mehanizmi in funkcionalnosti na požarni pregradi:**

* Možnost prepoznavanja in blokiranja prometa na nivoju aplikacij (vsaj: aplikacije za omogočanje oddaljene administracije, dostop do video vsebin, socialne medije, P2P, Anonymizer, škodljive aplikacije, visoko rizične aplikacije).
* Možnost pisanja pravil po državi (omejevanje dostopov do strežnika samo iz določenih držav).
* Prepoznavanje in filtriranje spletnih strani po vsebini (URL filtriranje).
* Omejevanje pasovne širine na osnovi zaznane aplikacije ali URL kategorije.
* Možnost posredovanja prometa na določen port (mirror interface)
* Možnost kreiranja lastnih kategorij in spreminjanje klasifikacije kategorije za določeno spletno stran.
* Proti-virusno pregledovanje prometa na osnovi že znanih signatur
* Zaznavanje in preprečevanje Botnet komunikacije in povezav do tako imenovanih »Command and control« strežnikov.
* Zaznavanje in preprečevanje DNS zahtev po imenih znanih »Command and control« strežnikov
* Možnost vključitve zaščite za odkrivanja in preprečevanje vdorov (IPS).
* Omogočena mora biti zaščita glede na lokacijo (državo) izvora prometa (GEO location protection).
* Pregledovanje HTTPS prometa:
  + rešitev mora podpirati uvoz priznanih kvalificiranih javnih potrdil
  + rešitev mora omogočati kreiranje izjem pri pregledovanju https prometa glede na: izvor prometa (uporabnik), cilj prometa (spletna stran ali kategorija)
  + kloniranje prometa
* Podpora anti-spam preverjanju na nivoju vzpostavitve SMTP seje.
* Preverjanje SMTP prometa v načinu MTA (mail transfer agent). Pregled zgodovine, trenutno stanje vrste e-pošte in izvedenih akcij
* Integriran ICAP klient in strežnik
* Podpora VPN povezavam z oddaljenimi partnerji.
* Ponudnik mora za 2. in 3. leto ponuditi varnostno zaščito:
  + Možnost podpore za preprečevanje okužb uporabnikov pred neznanimi virusi in novo zlonamerno kodo (zero day protection) ciljnih napadov.
  + Možnost podpore odstranjevanju še ne poznane zlonamerne kode vsebovane v aktivni vsebini dokumentov, kot so makro, vgrajeni objekti, itd… ter pošiljanje očiščene vsebine/dokumentov končnemu uporabniku v prvotni obliki ali pretvorjeno v pdf format.
  + Ponujena zaščita se mora izvajati v oblaku proizvajalca.

**3 kosi – Požarne pregrade nove generacije za oddaljene lokacije**

**Ponujeno:**

**Model \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Proizvajalec \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Oprema mora vključevati garancijo proizvajalca za čas trajanja pogodbe (tovarniška podpora za nadgradnjo in odpravo napak na strojni in programski opremi) za vso ponujeno strojno in programsko opremo.

**Minimalne zahtevane lastnosti strojne opreme za požarno pregrado (za posamezno napravo):**

* Velikost strojne opreme ne več kot 1 RU/ Desktop z možnostjo vgradnje v obstoječo komunikacijsko omaro
* Priključna vrata
  1. Najmanj 6x 10/100/1000Base-T RJ45 priključki
  2. USB ports 1 x USB3.0
* Napajanje 230 V AC
* Delovanje naprave v temperaturnem razponu od 0 do 40°C
* Skladnost z okoljskimi standardi kot so npr. ROHS II.
* Garancija proizvajalca: 3 leta, garantiran čas odprave strojne napake NBD

**Performančne zahteve požarne pregrade:**

* Prepustnost požarne pregrade vsaj 250Mbps realnega kriptiranega prometa (tipična Internetna protokolna distribucija, paketi z L7 vsebino, ter tipična distribucija velikost paketov – npr. IMIX) z vključenimi zahtevanimi varnostnimi mehanizmi.
* Število hkratnih sej preko požarne pregrade vsaj 100.000.
* Število novih sej na sekundo vsaj 10.000.

**Minimalne zahtevane lastnosti programske opreme – požarna pregrada:**

* Delovanje v L3 načinu (routing mode).
* Podpora za first hop redundancy protokol (VIP naslov za kliente).
* Sinhronizacija sej med člani gruče.
* »Stateful« požarna pregrada.
* Podpora mehanizmom za usmerjanje:
  + Statične route
  + Multicast route
  + OSPFv2 in v3
  + BGP
  + RIP
  + PIM-SM, PIM-SSM, PIM-DM
  + IGMP v2 in v3
* Podpora za IPv6 protokol:
  + Podpora funkcionalnostim: požarna pregrade, varnostno pregledovanje prometa (npr. URL filtering, IPS, blokiranje aplikacij)
* Integracija z aktivnim imenikom.
* Podpora centralnemu upravljanju in nadzoru
* Podpora centralnemu logiranju

**Zahtevani varnostni mehanizmi in funkcionalnosti na požarni pregradi:**

* Možnost prepoznavanja in blokiranja prometa na nivoju aplikacij (vsaj: aplikacije za omogočanje oddaljene administracije, dostop do video vsebin, socialne medije, P2P, Anonymizer, škodljive aplikacije, visoko rizične aplikacije).
* Možnost pisanja pravil po državi (omejevanje dostopov do strežnika samo iz določenih držav).
* Prepoznavanje in filtriranje spletnih strani po vsebini (URL filtriranje).
* Omejevanje pasovne širine na osnovi zaznane aplikacije ali URL kategorije.
* Možnost posredovanja prometa na določen port (mirror interface)
* Možnost kreiranja lastnih kategorij in spreminjanje klasifikacije kategorije za določeno spletno stran.
* Proti-virusno pregledovanje prometa na osnovi že znanih signatur
* Zaznavanje in preprečevanje Botnet komunikacije in povezav do tako imenovanih »Command and control« strežnikov.
* Zaznavanje in preprečevanje DNS zahtev po imenih znanih »Command and control« strežnikov
* Možnost vključitve zaščite za odkrivanja in preprečevanje vdorov (IPS).
* Omogočena mora biti zaščita glede na lokacijo (državo) izvora prometa (GEO location protection).
* Pregledovanje HTTPS prometa:
  + rešitev mora podpirati uvoz priznanih kvalificiranih javnih potrdil
  + rešitev mora omogočati kreiranje izjem pri pregledovanju https prometa glede na: izvor prometa (uporabnik), cilj prometa (spletna stran ali kategorija)
  + kloniranje prometa
* Podpora anti-spam preverjanju na nivoju vzpostavitve SMTP seje.
* Preverjanje SMTP prometa v načinu MTA (mail transfer agent). Pregled zgodovine, trenutno stanje vrste e-pošte in izvedenih akcij
* Integriran ICAP klient in strežnik
* Podpora VPN povezavam z oddaljenimi partnerji.

Vseh 5 kosov požarnih pregrad se upravlja z obstoječim centralnim upravljalnim sistemom (Check Point).

**Produkti / funkcionalnosti**

|  |  |
| --- | --- |
| **Koda** | **Opis** |
| CPSM-NGSM5 | Next Generation Security Management Software for 5 gateways (SmartEvent) 1 year |
| CPSB-EVS-5-2Y | SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & open server) 2 year subscription |
| CPSB-NGFW-5400-3Y | Next Generation Firewall Package subscription for 3 year for 5400 Appliance |
| CPSB-NGFW-5400-3Y-HA | Next Generation Firewall Package subscription for 3 year for 5400 Appliance HA |

**Podpora proizvajalca (Support)**

|  |  |
| --- | --- |
| **Koda** | **Opis** |
| CPSM-NGSM5 | Standard Collaborative Enterprise Support |
| CPAP-SG5400-NGTP | Standard Collaborative Enterprise Support |
| CPAP-SG5400-NGTP-HA | Standard Collaborative Enterprise Support |
| CPSB-MOB-50 | Standard Collaborative Enterprise Support |
| CPSB-MOB-50-HA | Standard Collaborative Enterprise Support |

Spodaj podpisani pooblaščeni predstavnik ponudnika izjavljam, da vsa ponujena oprema v celoti ustreza zgoraj navedenim opisom.

V/na \_\_\_\_\_\_\_\_\_\_\_, dne \_\_\_\_\_\_\_\_\_\_

Ime in priimek:

Žig in podpis: