**Trenutno okolje:**

**V naročnikovem okolju so trenutno postavljene požarne pregrade proizvajalca PaloAlto PA-3020 s funkiconalnostmi GlobalProtect za varno oddaljeno povezavo mobilnih uporabnikov (IPSec/SSL VPN), Threat prevention, Wildfire in URL filtering. Požarni pregradi PA-3020 sta postavljeni v HA načinu Active/Passive.**

**Opremo bomo nadgradili zaradi objave proizvajalca o koncu podpore in življenjske dobe trenutnih produktov (End-od-life) in ker želimo ohraniti obstoječo stopnjo varnosti (funkcionalnosti) omrežja in jo dopolniti s strojnim učenjem varnostnih naprav, ki bodo lahko samodejno prepoznavale obnašanje naprav v omrežju in možne napade. Doda se še funkcionalnost DNS Security za zaščito pred napadi/vdori, ki izkoriščajo omrežje DNS.**

|  |  |  |
| --- | --- | --- |
| **Požarna pregrada naslednje generacije PAN-PA-3220 z naslednjimi karakteristikami:** | | **Količina : 2** |
| **Osnovne zahteve** | * Prepustnost pri preverjanju nevarnosti (Threat prevention) vsaj 2,8 Gbps * Najmanj 12x 10/100/1000 vmesnikov * Najmanj 4x 1 G SFP, 4x 1G/10G SFP/SFP+ vmesnikov * Vsaj 2x 10/100/1000 high availability in 1x 10G SFP+ high availability vmesnik, * Najmanj 1x 10/100/1000 Out-of-band vmesnik za upravljanje * Interna kapaciteta diska najmanj 240 GB SSD * Možnost HA (visoka razpoložljivost) načina delovanja (active/active) * Podpora za različne načine delovanja:   + L2, L3 nivo   + TAP mode   + Virtual wire (transparent mode) * Usmerjanje:   + Podpora za OSPF, RIP, BGP   + Forwarding table size (per device/per VR): 2500/2500 ali več   + Policy-based forwarding   + PPPoE   + Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, v3   + Podpora za IPv6 (L2, L3, TAP mode, virtual wire) * VLANs   + 802.1q VLAN tags per device/per interface 4094/4094 ali več   + MAX Intefraces: 4096 ali več   + 802.3ad * L2 preusmerjanje (forwarding)   + ARP table size/device 16000   + MAC table size/device 16000   + IPv6 table size/device 16000 * Varnost   + Policy-based control over applications, users and content   + DoS/DDos protection   + Decryption: SSL (inbound and outbound), SSH     - Indentifikacija in kontrola prometa na aplikativnem nivoju, ne glede na vrata, protokol ali enkripcijo (SSL – inbound in outbound, SSH) * Lasten operacijski sistem * Algoritmi strojnega učenja (machine learning) za napredno zaščito direktno na napravi brez zunanjih povezav * Možnost kreiranja varnostnih politik za preprečevanje kraje poverilnic * Podpirati mora dinamično in samodejno regrupacijo uporabnika/ov glede na varnostne incidente povezane s tem uporabnikom/ki * Grafična analiza prometa * Sposobnost integracije za MS AD, LDAP, eDirectory | |
| **Dodatne zahteve** | * Licenca za preprečevanje zlonamernih vdorov in groženj (kot »Palo Alto Threat Prevention subscription«) * Licenca za prepoznavo in preprečevanje novih neznanih groženj (kot »Palo Alto Wildfire Subscription«) * Licenca za filtriranje URL prometa (kot »Palo Alto PANDB URL Filtering Subscription«) * Licenca za dostop mobilnih uporabnikov do lokalnega omrežja (kot »PaloAlto Global protect subscription«) * Licenca za nadzor DNS prometa (kot »PaloAlto DNS Security subscription«) | |

|  |  |  |
| --- | --- | --- |
| **Požarna pregrada naslednje generacije PAN-PA-220 z naslednjimi karakteristikami:** | | **Količina : 1** |
| **Osnovne zahteve** | * Vrsta ohišja desktop * Prepustnost pri preverjanju nevarnosti (Threat prevention) 320 Mbps * Najmanj 8 10/100/1000 vmesnikov * Najmanj 1x 10/100/1000 Out-of-band vmesnik za upravljanje * Interna kapaciteta diska najmanj 32 GB eMMC * Možnost HA (visoka razpoložljivost) načina delovanja (active/active) * Podpora za različne načine delovanja:   + L2, L3 nivo   + TAP mode   + Virtual wire (transparent mode) * Usmerjanje:   + Podpora za OSPF, RIP, BGP   + Forwarding table size (per device/per VR): 1000/1000 ali več   + Policy-based forwarding   + PPPoE   + Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, v3   + Podpora za IPv6 (L2, L3, TAP mode, virtual wire) * VLANs   + 802.1q VLAN tags per device/per interface 4094/4094 ali več   + MAX Intefraces: ali več 1024   + 802.3ad * NAT/PAT   + Podpora za vsaj 400 NAT pravil (NAT rules)   + Podpora za vsaj 200 NAT DIPP pravil (NAT DIPP rules)   + NAT modes: 1:1 NAT, n:n NAT, m:n NAT * MAX Virtual wires 256 ali več * L2 preusmerjanje (forwarding)   + ARP table size/device 1500   + MAC table size/device 1500   + IPv6 table size/device 1500 * Varnost   + Policy-based control over applications, users and content   + DoS/DDos protection   + Decryption: SSL (inbound and outbound), SSH     - Indentifikacija in kontrola prometa na aplikativnem nivoju, ne glede na vrata, protokol ali enkripcijo (SSL – inbound in outbound, SSH) * Lasten operacijski sistem * Algoritmi strojnega učenja (machine learning) za napredno zaščito direktno na napravi brez zunanjih povezav * Možnost kreiranja varnostnih politik za preprečevanje kraje poverilnic * Podpirati mora dinamično in samodejno regrupacijo uporabnika/ov glede na varnostne incidente povezane s tem uporabnikom/ki * Grafična analiza prometa * Sposobnost integracije za MS AD, LDAP, eDirectory * Identifikacija CITRIX XenApp, MS Terminal Services uporabnikov | |
| **Dodatne zahteve** | * Licenca za preprečevanje zlonamernih vdorov in groženj (kot »Palo Alto Threat Prevention subscription«) * Licenca za filtriranje URL prometa (kot »Palo Alto PANDB URL Filtering Subscription«) | |
| **Implementacija požarnih pregrad v naročnikovo okolje** | | **Količina : 1** |
| **Storitve implementacije** | * Dobava opreme in konfiguracija osnovnih nadzornih parametrov * Posodobitev strojne kode na od proizvajalca priporočeno verzijo * Priklop na komunikacijsko omrežje naročnika * Prenos konfiguracije iz obstoječih požarnih pregrad na nove požarne pregrade * Registracija ustreznih funkcijskih modulov * Integracija z MS aktivnim imenikom * Ureditev potrebne VLAN infrastrukture glede na obstoječe omrežje * Priprava avtomatiziranja posodobitev funkcijskih modulov * Sledenje in tipiziranje tekočega prometa po posameznih nadzornih sklopih * Definicija potrebnih aplikacijskih filtrov po posameznih nadzornih sklopih * Postopno uvajanje IPS funkcionalnosti znotraj nadzornih sklopov   + Izdelava poročil po zahtevah naročnika   + Nastavitev VPN oddaljenega dostopa z identifikacijo uporabnikov preko MS AD (LDAP, NPS …) * Testiranje delovanja * Uvajanje sistemskega administratorja in predaja sistema (4 ure) * Predaja v produkcijo | |

**Skupne zahteve:**

* Vsa ponujena strojna oprema mora biti od istega proizvajalca,
* Izjavo proizvajalca, da dobavljena oprema v trenutku prevzema nima vgrajenih implantatov (implants), ki omogočajo nepooblaščeno prestrezanje prometa ali nadzor nad opremo, ki je predmet nakupa.
* Ponudnik mora imeti partnerski status za ponujeno rešitev,
* Vsi servisni paketi za vzdrževanje, nadgradnjo in podporo opreme morajo biti od proizvajalca strojne oz. programske opreme
  + Garancija za celotno strojno in programsko opremo ter podpora mora biti 36 mesecev na lokaciji naročnika
  + Odzivnost : 24ur na dan, vse dni v tednu (24x7 za Critical errors)
  + Telefonski odzivni čas (CALL Response Time):
    - Critical: manj kot 1h
    - High: največ 2 uri
    - Medium: največ 4 ure
    - Low: največ 8 ur