

**Tehnička specifikacija za nabavu i implementaciju sustava
vatzrozida za podatkovni centar u Zagrebu i Rijeci
Ev. Br. 7-VV-24**

Sadržaj

1.	Uvod	3
1.1.	Cilj projekta/postupka nabave	3
1.2.	Opis postojećeg stanja	3
2.	Opis predmeta nabave	4
2.1.	Općeniti pregled	4
2.2.	Zahtjevi za sustav vatrozida u podatkovnom centru na primarnoj lokaciji- Palo Alto Neteworks PA-3420 ili jednakovrijedan.....	5
2.3.	Zahtjevi za virtualni vatrozid za DR lokaciju – PAN-SOFTWARE-NGFW-CR ili jednakovrijedan.....	10
3.	Usluga instalacije i Implementacije vatrozid sustava.....	14
3.1.	Isporuke koje se očekuju tijekom provedbe ovog projekta	14

1. Uvod

1.1. Cilj projekta/postupka nabave

Cilj javne nabave je provesti nabavu i aktivnosti kako bi se zamijenili postojeći PA-5050 vatrozidi u podatkovnim centrima sa novim modelima. Naručitelj je planirao provesti izmjenu postojećih vatrozida obzirom da se radi o starijim uređajima za koje proizvođač prestaje pružati podršku i resurse za održavanje. Obzirom da se radi o sigurnosno ključnim resursima Informacijskog sustava Naručitelja potrebna je obnova.

Prilikom zamjene vatrozida planirano je provesti nabavu fizičkih uređaja za primarni podatkovni centar i virtualne uređaje za rezervni podatkovni centar. I za jednu i za drugu lokaciju potrebno je osigurati visoku dostupnost i pouzdanost u radu što će se postići nabavom uređaja u paru (redundantni uređaji). Izmjenom uređaja i u primarnom i rezervnom podatkovnom centru naručitelj želi osigurati i olakšati aktivnosti prilikom aktivnog rada rezervne lokacije ili potpunog posluživanja servisa sa rezervne lokacije.

Izmjenom vatrozida naručitelj planira održati i podići razinu sigurnosti infrastrukture informacijskog sustava Carinske uprave i dodatno zaštiti promet na razini aplikacija i korisnika.

Dovršetkom javne nabave i projektom implementacije po potpisanim ugovorima Naručitelj očekuje provedenu izmjenu postojećih zastarjelih uređaja novima, nove uređaje u potpuno operativnom radu integrirane u Informacijski sustav Carinske uprave u primarnom i rezervnom podatkovnom centru.

1.2. Opis postojećeg stanja

Postojeći vatrozidi PA-5050 smješteni u primarnom podatkovnom centru proizvedeni su od strane Palo Alto Networks koji je objavio da prestaje davati podršku za tu seriju uređaja, te da prestaje izdavati kritične nadogradnje zaključno sa 30.01.2024. godine. Nakon tog datuma više neće biti moguće provesti nadogradnju softvera uređaja, prijaviti grešku proizvođaču i zatražiti pomoć u slučaju problema u radu vatrozida ili napraviti zamjenu uređaja u slučaju kvara.

Isto tako postojeći vatrozidi imaju zastarjeli operativni sustav i nemaju mogućnost detekcije i blokiranja naprednih tehnika napadača.

Postojeći vatrozidi implementirani su na kritičnoj točci sustava (ulaz i izlaz iz podatkovnog centra, Informacijskog sustava Carinske uprave) te se bilo kakav problem u radu vatrozida direktno odražava se na dostupnost i stabilnost ovog dijela informacijskog sustava. Iz navedenog vatrozide je planirano zamijeniti novim modelima.

2. Opis predmeta nabave

2.1. Općeniti pregled

Potrebno je nabaviti, dopremiti i u Informacijski sustav Carinske uprave integrirati četiri nova vatrozid uređaja. Dva fizička za primarni podatkovni centar i dva virtualna za rezervni podatkovni centar.

Novi uređaji moraju u potpunosti zamijeniti postojeće uređaja. Na novim uređajima potrebno je uspostaviti i rekonstruirati sve postojeće promete i politike sa aktualnih uređaja.

Prije instalacije potrebno je napraviti analizu prometa te plan migracije servisa na nove uređaja uz provedbu analize rizika migracije i utjecaj na poslovanje.

Novi vatrozidi moraju imati operativni sustav sa modulom za strojno učenje koji omogućuje sljedeće funkcionalnosti za blokiranje naprednih prijetnji:

- prevenciju i sprječavanje zero day napada u realnom vremenu
- prevencija i detekcija nepoznatih exploit-a i C2 alata
- prevencija i detekcija Cobalt strike framework-a
- detekcija i prevencija OWASP Top 10 tehnika poput SQL i komandnih injekcija.

Vatrozidi moraju omogućiti potpunu vidljivost zlonamjernog ponašanja te identifikaciju prijetnji u cjelokupnom prometu kao i detektiranje fileless prijetnji, a korištenjem „sandbox“ analiza prijetnji moraju spriječiti napade u stvarnom vremenu.

Vatrozidi moraju imati mogućnost čitanja sadržaja DNS paketa, te sukladno tome odraditi blokiranje ili preusmjeravanje DNS odgovora koji u sebi sadrže maliciozne domene, te blokiranje DNS tuneliranja.

Vatrozidi moraju imati IPS koji nije vezan isključivo uz bazu IPS signaturea, nego može u realnom vremenu, korištenjem algoritama strojnog učenja, zaključiti da je neki promet maliciozan i blokirati ga (iako nema predefiniran signature za tu prijetnju), te mora odraditi filtriranje i blokiranje prijenosa datoteka ovisno o vrsti datoteke.

2.2. Zahtjevi za sustav vatrozida u podatkovnom centru na primarnoj lokaciji- Palo Alto Networks PA-3420 ili jednakovrijedan

Zahtijevane karakteristike	Obavezno/opcija	Sukladnost tehničkoj specifikaciji (DA/NE)
Rješenje mora biti visoko dostupna skalabilna arhitektura s 2 poslužitelja. Svaki od poslužitelja mora biti opremljen sa redundantnim napajanjima (redundant AC power supplies).	Obavezno	
Sustav vatrozida mora biti hardversko rješenje	Obavezno	
Upravljački sustav mora biti integriran	Obavezno	
Broj sučelja mora biti minimalno 26, od čega: - Minimalno 12 1/2.5/5/10Gbps RJ-45 sučelja, - Minimalno 10 1/10Gbps SFP/SFP+ sučelja. - Minimalno 4 25G SPF+ sučelja	Obavezno	
Ugrađeno minimalno jedno 10/100/1000 Mbps RJ-45 Ethernet sučelje za udaljeno upravljanje	Obavezno	
Ugrađeno minimalno jedno serijsko sučelje za upravljanje (konzola)	Obavezno	
Ugrađen minimalno jedan Solid-State disk od 480 GB	Obavezno	
Mogućnost ugradnje u 19" komunikacijski ormari, najveća veličina uređaja 1RU	Obavezno	
Minimalna propusnost vatrozida s uključenom funkcijom prepoznavanja i kontrole aplikacija je 16.9 Gbps	Obavezno	
Minimalna propusnost vatrozida s uključenim naprednim funkcionalnostima (kontrola i vidljivost aplikacija, IPS) je 7.6 Gbps	Obavezno	

Minimalna propusnost za 3DES/AES VPN promet je 9.9 Gbps	Obavezno	
Minimalni podržani broj istovremenih sesija je 2.000.000	Obavezno	
Minimalni broj novih sesija po sekundi 205.000	Obavezno	
Minimalni podržani broj istovremenih VPN LAN-to-LAN konekcija je 5.000	Obavezno	
Minimalno podržano 1800 istovremenih klijentskih VPN konekcija	Obavezno	
Klijentske konekcije je moguće ostvariti s računala koja imaju Microsoft Windows 7 i Windows 10 operacijske sustave	Obavezno	
Podrška za active/standby i active/active način rada radi osiguranja redundancije	Obavezno	
Upravljački sustav je integriran u vatrozid	Obavezno	
U upravljačkom sustavu mora biti integriran sustav za izvještavanje sa skupom predefiniranih izvještaja na način da postoji: - Mogućnost kreiranja detaljnih izvještaja o korisničkim aktivnostima. - Mogućnost automatske izrade izvještaja. - Mogućnost automatskog slanja izvještaja na e-mail adrese administratora.	Obavezno	
Podrška za neograničen broj korisnika	Obavezno	
Podrška za rad vatrozida u L2 i L3 načinu rada	Obavezno	
Podrška za potpuno transparentan (virtual-wire) način rada	Obavezno	
Mogućnost implementacije vatrozida u Tap načinu rada	Obavezno	
Podrška za 802.1Q trunking protokol i izradu subinterfacea	Obavezno	
Podrška za agregiranje Ethernet sučelja korištenjem LACP protokola	Obavezno	
Podrška za upravljanje administratorskim korisničkim računima, mogućnost integracije sa sustavima za upravljanje korisnicima putem TACACS+, RADIUS, LDAP, KERBEROS, SAML protokola	Obavezno	
Podrška za autentikaciju i autorizaciju VPN korisnika korištenjem RADIUS, LDAP,	Obavezno	

KERBEROS, SAML protokola – mogućnost integracije s vanjskim sustavima za upravljanje korisnicima		
Podrška za multi-faktorsku autentikaciju	Obavezno	
Podrška za udaljeni administratorski pristup SSHv2 i HTTPS protokolima	Obavezno	
Podrška za SNMP protokol verzije 3	Obavezno	
Podrška za slanje syslog poruka	Obavezno	
Podrška za slanje informacija o prometu kroz vatrozid (NetFlow ili jednako vrijedan protokol)	Obavezno	
Podrška za sljedeće usmjerivačke protokole: OSPF, RIP, BGP, ECMP, BFD	Obavezno	
Podrška za minimalno 11 istovremenih usmjerivačkih tablica	Obavezno	
Podrška za PBF (Policy Based Forwarding) na temelju IP adresa, aplikacija i korisničkih informacija	Obavezno	
Podrška za NAT i PAT	Obavezno	
Podrška za QoS	Obavezno	
Mogućnost klasificiranja i ograničavanja prometa na temelju aplikacija, URL kategorija i korisničkih informacija, te DSCP i ToS vrijednosti	Obavezno	
Podrška za DoS zaštitu vatrozida i zona koje vatrozid osigurava	Obavezno	
Mogućnost kreiranja virtualnih vatrozida koja se može, ukoliko će naknadno trebati, otključati licencom	Obavezno	
Podrška za kreiranje pravila na temelju IP adresa, aplikacija, korisničkog imena ili grupe, URL kategorije	Obavezno	
Mogućnost povezivanja vatrozida s Microsoft Active Directory imeničkim servisom (bez korištenja dodatnog klijenta)	Obavezno	
Mogućnost integracije s Microsoft Remote Desktop serverima kako bi e identificirali korisnici koji su spojeni na te servere	Obavezno	

Mogućnost presretanja HTTP korisničkog prometa i autentikacije korisnika putem integriranih portala	Obavezno	
Vatrozid posjeduje Common Criteria i FIPS 140-2 certifikate	Obavezno	
Podrška za multicast promet	Obavezno	
Podrška za REST API ili jednakovrijedan protokol	Obavezno	
Podrška za TLS 1.2 za SSL VPN pristup	Obavezno	
Podrška za IKEv1 i IKEv2 IPSec protokole	Obavezno	
Integriran Intrusion Protection System (IPS), bez dodatne programske ili hardverske instalacije, koji se otključava licencom	Obavezno	
Integrirana anti-spyware i anti-virusna zaštita, bez dodatne programske ili hardverske instalacije, koja se otključava licencom	Obavezno	
Mogućnost detekcije aplikacija neovisno o portovima koje aplikacija koristi	Obavezno	
Mogućnost izrade custom (korisničkih) aplikacija	Obavezno	
Automatski download novih aplikacija. Mogućnost analize utjecaja novih aplikacija na postojeću konfiguraciju sigurnosnih pravila	Obavezno	
Mogućnost ispitivanja DNS upita i blokiranja upita prema malicioznim domenama za neograničen broj upita i korisnika. Funkcionalnost se mora otključati licencom	Obavezno	
Mogućnost ispitivanja URL-ova i mogućnost blokiranja URL-ova na temelju kategorija. Funkcionalnost se mora otključati licencom	Obavezno	
Podrška za X-Forwarded-For polja u zaglavljima paketa. Mogućnost micanja tog polja prije proslijeđivanja paketa na Internet	Obavezno	
Mogućnost kreiranja korisničkih (custom) URL kategorija	Obavezno	
Mogućnost dekripcije SSL prometa	Obavezno	
Mogućnost filtriranja i blokiranja minimalno sljedećih datoteka: 7z, bat, cab, chm, class, cpl,	Obavezno	

dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf, enkriptirani rar i enkriptirani zip		
Mogućnost blokiranja nakon detektiranja tih uzoraka	Obavezno	
Automatski download baza novih IPS, anti-virus i anti-spyware potpisa	Obavezno	
Implementirana anti-malware zaštita sa sandboxing funkcionalnošću, koja se otključava licencama	Obavezno	
Mogućnost konfiguracije limita za veličinu različitih vrsta datoteka koje se šalju na analizu u sandboxing sustav	Obavezno	
Mogućnost odabira dodatnih informacija koje se šalju u sandboxing sustav	Obavezno	
Sustav mora osiguravati analizu bez utjecaja na performanse sustava kao npr. kašnjenje u mrežnoj komunikaciji	Obavezno	
Sustav mora biti u mogućnosti identificirati maliciozni sadržaj s nastojanjem da broj false-positive alarma bude vrlo mali ili zanemariv	Obavezno	
Threat Prevention podrška u trajanju od 3 godine za uređaje u HA, par, PA-3420 (PAN-PA-3420-ATP-3YR-HA2-Advanced), za 2 uređaja	Obavezno	
Napredna WildFire podrška po uređaju u HA režimu rada, par, u trajanju od 3 godine (36 mjeseci), (PAN-PA-3420-AWF-3YR-HA2-PA-3420) za 2 uređaja	Obavezno	
Pružanje premium podrške u trajanju od 3 godine (term), (PAN-SVC-BKLN-3420-3YR-Partner), za 2 uređaja	Obavezno	
Jamstveni rok – minimalno 3 godine, koji uključuje i programske nadogradnje svih komponenti te nadogradnje baze IPS i AV potpisa te mogućnost sandboxing inspekcije prometa	Obavezno	

2.3. Zahtjevi za virtualni vatrozid za DR lokaciju – PAN-SOFTWARE-NGFW-CR ili jednakovrijedan

Zahtijevane karakteristike	Obavezno/opcija	Sukladnost tehničkoj specifikaciji (DA/NE)
Ponuđeni vatrozid mora biti softversko rješenje koje uključuje i NGFW Credits to deploy VM-Series, CN-Series, Subscription Services, and Virtual Panorama to manage Software Firewalls. (PAN-SOFTWARE-NGFW-CR-Software), 26 komada	Obavezno	
Upravljački sustav mora biti integriran	Obavezno	
Minimalna propusnost vatrozida s uključenom funkcijom prepoznavanja i kontrole aplikacija je 5 Gbps	Obavezno	
Minimalna propusnost vatrozida s uključenim naprednim funkcionalnostima (kontrola i vidljivost aplikacija, IPS) je minimalno 3 Gbps	Obavezno	
Minimalni podržani broj istovremenih sesija je 500 000	Obavezno	
Minimalni broj novih sesija po sekundi 30 000	Obavezno	
Minimalni podržani broj istovremenih VPN LAN-to-LAN konekcija je 1000	Obavezno	
Podrška za active/standby i active/active način rada radi osiguranja redundancije	Obavezno	
Upravljački sustav je integriran u vatrozid	Obavezno	
U upravljačkom sustavu mora biti integriran sustav za izvještavanje sa skupom predefiniranih izvještaja	Obavezno	
Mogućnost kreiranja detaljnih izvještaja o korisničkim aktivnostima	Obavezno	
Mogućnost automatske izrade izvještaja	Obavezno	
Mogućnost automatskog slanja izvještaja na e-mail adrese administratora	Obavezno	

Podrška za neograničen broj korisnika	Obavezno	
Podrška za rad vatrozida u L3 načinu rada	Obavezno	
Podrška za 802.1Q trunking protokol i izradu subinterfacea	Obavezno	
Podrška za upravljanje administratorskim korisničkim računima, mogućnost integracije sa sustavima za upravljanje korisnicima putem TACACS+, RADIUS, LDAP, KERBEROS, SAML protokola	Obavezno	
Podrška za autentikaciju i autorizaciju VPN korisnika korištenjem RADIUS, LDAP, KERBEROS, SAML protokola – mogućnost integracije s vanjskim sustavima za upravljanje korisnicima	Obavezno	
Podrška za multi-faktorsku autentikaciju	Obavezno	
Podrška za udaljeni administratorski pristup SSHv2 i HTTPS protokolima	Obavezno	
Podrška za SNMP protokol verzije 3	Obavezno	
Podrška za slanje syslog poruka	Obavezno	
Podrška za slanje informacija o prometu kroz vatrozid (NetFlow ili jednako vrijedan protokol)	Obavezno	
Podrška za sljedeće usmjerivačke protokole: OSPF, RIP, BGP, ECMP, BFD	Obavezno	
Podrška za minimalno 10 istovremenih usmjerivačkih tablica	Obavezno	
Podrška za PBF (Policy Based Forwarding) na temelju IP adresa, aplikacija i korisničkih informacija	Obavezno	
Podrška za NAT i PAT	Obavezno	
Podrška za QoS	Obavezno	
Mogućnost klasificiranja i ograničavanja prometa na temelju aplikacija, URL kategorija i korisničkih informacija, te DSCP i ToS vrijednosti	Obavezno	
Podrška za DoS zaštitu vatrozida i zona koje vatrozid osigurava	Obavezno	

Podrška za kreiranje pravila na temelju IP adresa, aplikacija, korisničkog imena ili grupe, URL kategorije	Obavezno	
Mogućnost povezivanja vatrozida s Microsoft Active Directory imeničkim servisom (bez korištenja dodatnog klijenta)	Obavezno	
Mogućnost integracije s Microsoft Remote Desktop serverima kako bi e identificirali korisnici koji su spojeni na te servere	Obavezno	
Mogućnost presretanja HTTP korisničkog prometa i autentikacije korisnika putem integriranih portala	Obavezno	
Vatrozid posjeduje Common Criteria i FIPS 140-2 certifikate	Obavezno	
Podrška za multicast promet	Obavezno	
Podrška za REST API ili jednakovrijedan protokol	Obavezno	
Podrška za TLS 1.2 za SSL VPN pristup	Obavezno	
Podrška za IKEv1 i IKEv2 IPsec protokole	Obavezno	
Integriran Intrusion Protection System (IPS), bez dodatne programske ili hardverske instalacije, koji se otključava licencom	Obavezno	
Integrirana anti-spyware i anti-virusna zaštita, bez dodatne programske ili hardverske instalacije, koja se otključava licencom	Obavezno	
Mogućnost detekcije aplikacija neovisno o portovima koje aplikacija koristi	Obavezno	
Mogućnost izrade custom (korisničkih) aplikacija	Obavezno	
Automatski download novih aplikacija	Obavezno	
Mogućnost analize utjecaja novih aplikacija na postojeću konfiguraciju sigurnosnih pravila	Obavezno	
Mogućnost ispitivanja DNS upita i blokiranja upita prema malicioznim domenama za neograničen broj upita i korisnika. Funkcionalnost se mora otključati licencom	Obavezno	

Mogućnost ispitivanja URL-ova i mogućnost blokiranja URL-ova na temelju kategorija. Funkcionalnost se mora otključati licencom	Obavezno	
Podrška za X-Forwarded-For polja u zaglavljima paketa. Mogućnost micanja tog polja prije prosljeđivanja paketa na Internet	Obavezno	
Mogućnost kreiranja korisničkih (custom) URL kategorija	Obavezno	
Mogućnost dekripcije SSL prometa	Obavezno	
Mogućnost filtriranja i blokiranja minimalno sljedećih datoteka: 7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf, enkriptirani rar i enkriptirani zip	Obavezno	
Mogućnost kreiranja uzoraka (patterna) i pretraživanja svih paketa na te uzorke. Mogućnost blokiranja nakon detektiranja tih uzoraka	Obavezno	
Automatski download baza novih IPS, anti-virus i anti-spyware potpisa	Obavezno	
Implementirana anti-malware zaštita sa sandboxing funkcionalnošću, koja se otključava licencama	Obavezno	
Mogućnost konfiguracije limita za veličinu različitih vrsta datoteka koje se šalju na analizu u sandboxing sustav	Obavezno	
Mogućnost odabira dodatnih informacija koje se šalju u sandboxing sustav	Obavezno	
Sustav mora osiguravati analizu bez utjecaja na performanse sustava kao npr. kašnjenje u mrežnoj komunikaciji	Obavezno	
Sustav mora biti u mogućnosti identificirati maliciozni sadržaj s nastojanjem da broj false-positive alarma bude vrlo mali ili zanemariv	Obavezno	
Jamstveni rok – minimalno 3 godine, koji uključuje i programske nadogradnje svih komponenti te nadogradnje baze IPS i AV potpisa	Obavezno	

3. Usluga instalacije i Implementacije vatrozid sustava

- Odabrani Ponuditelj dužan je provesti nabavu, instalaciju i integraciju tehničkog rješenja u Informacijski sustav Carinske uprave.
- Nakon isporuke komponenti vatrozid sustava (fizičkih komponenti, softverskih komponenti i pripadajućih licenci) administratori ponuditelja dužni su provesti postavljanje uređaja na infrastrukturi i okruženju Carinske uprave.
- Po provedenoj ugradnji administratori ponuditelja moraju provesti instalaciju, konfiguraciju i integraciju opreme u infrastrukturnom okruženju Carinske uprave, i nakon toga dužni su provesti odgovarajuće testiranje, izraditi tehničku dokumentaciju izvedenog stanja, i opremu pustiti u produksijski rad sukladno definiranoj LLD shemi i arhitekturi sustava.

3.1. Isporuke koje se očekuju tijekom provedbe ovog projekta

- Izraditi plan upravljanja projektom koji sadrži organizacijsku strukturu projekta i načine komunikacije članova projektnog tima
- Izraditi projektni plan koji će minimalno uključivati ključne točke projekta: isporuka, termine instalacije i integracija, testiranja i puštanja u produkciju
- Izraditi tehničku specifikaciju zahtijevane arhitekture sustava
- Dokumentirati izvedeno stanje (evidencija opreme s pripadajućim konfiguracijama i lokacijama instalacije)
- Prezentirati izvedeno stanje i rezultate projekta predstavnicima Naručitelja