ЈАВНО ПРЕДУЗЕЋЕ ЕЛЕКТРОПРИВРЕДА СРБИЈЕ БЕОГРАД
Улица Царице Милице 2
Београд
Број: 12.01-8461/43-17
Датум: 02.02.2017. године

На основу члана 54. и 63. Закона о јавним набавкама („Службени гласник РС", број 124/12, 14/15 и 68/15), Комисија за јавну набавку број ЈН/1000/0201/2016, за набавку добара: Рачунарска опрема, по партијама, на захтев заинтересованог лица, даје

ДОДАТНЕ ИНФОРМАЦИЈЕ ИЛИ ПОЈАШЊЕЊА
У ВЕЗИ СА ПРИПРЕМАЊЕМ ПОНУДЕ,
РЕДНИ БРОЈ НАБАВКЕ ЈН/1000/0201/2016
Бр. 17

Пет и више дана пре истека рока предвиђеног за подношење понуда, заинтересовано лице је у писаном облику од наручиоца тражило додатне информације односно појашњења а Наручилац у року од три дана од дана пријема захтева даје следеће информације, односно појашњења:

ПИТАЊЕ 1:
На страни 29/159 у техничкој спецификацији за Партију 9. FIREWALL, МОЛИМ Вас да одговорите које функционалности уређај треба да обезбеди (типа antivirus, spyware protection, intrision prevention...deep packet inspection, conetent filetering?

ОДГОВОР 1:

Neophodne Firewall funkcionalnosti:
Osnovne Internet gateway funkcionalnosti kroz firewall, mrežne alate i servise, rutiranje, NAT, omogućavanje udaljenog korisničkog VPN pristupa mreži putem PPTP, L2TP, IPSEC i SSL protokola i omogućavanje site-to-site VPN konekcija putem IPSEC i SSL protokola.
Blokiranje saobraćaja po državama/kontinentima (inbound/outbound), color coded grupisanje firewall polisa, time based firewall polise (polise koje su definisane vremenom).
Neophodne Network Protection funkcionalnosti:
Detekcija i sprečavanje sofisticiranih napada koje firewall ne može sam zaustaviti.
Konfigurativni Intrusion Protection System (IPS) i Flood Protection protiv denial of service (DoS) napada.
Podrška za Cisco VPN klijente, clientless vpn pristup za sledeće protokole (RDP, VNC, Telnet, HTTP/S), Plug 'n' play site to site konekcija putem hardware-a uređaja istog proizvođača.
Podrška za uplink failover koristeći UMTS/3G USB stick.
One time password funkcionalnost koja je integrisana na uređaju bez kupovine dodatne licence (OTP) kao i podrška za hardverski OTP token.
Mogućnost da korisnici sami download-uju SSL VPN klijenta sa portala koji se nalazi na samom uređaju.
Podrška za IPv6, VLAN tagging, podrška za link agregaciju, WAN uplink balancing, dinamičko rutiranje (OSPF, BGP), mogućnost kreiranja DHCP servera za svaki interfejs na uređaju, podrška za QoS (određivanje garantovanog i maksimalnog protoka za aplikacije i protokole).

Neophodne Web Protection funkcionalnosti

Zaštita klijenata od web pretnji kroz dual anti-virus engine i kontrola njihovog pristupa web sadržaju. Mogućnost detekcije i ograničavanja korišćenja neželjenih aplikacija zbog veće sigurnosti i štednje resursa neophodnih za poslovne potrebe.
Mogućnost inspekcije HTTPS saobraćaja.
Mogućnost korišćenja transparent moda sa autentifikacijom (AD, Browser).
Mogućnost korišćenja Full Transparent proxy moda, mogućnost podešavanja upstream proxy-a (parent proxy) u zavisnosti od Source IP adrese, user/grupe, vremena, domena i URL-a.
Mogućnost korišćenja HTTP Proxy PAC file-a na samom uređaju.
Korišćenje cache-iranja na samom uređaju bez dodatne licence.
Integrisana dva antivirus engine-a različitih proizvođača.
Podrška za Active Directory SSO, Apple open directory SSO, basic user, browser i eDirectory SSO autentifikaciju, mogućnost autentifikacije po operativnom sistemu (Windows, MAC OS X, Kindle, Blackberry).
Korisćenje različitih vrsta autentifikacije za različite mrežne segmente.
Mogućnost važenja polisa po vremenu/danima.
Mogućnost filtriranja web saobraćaja po kategorijama sajtova (minimum 90).
Omogućavanje ili blokiranje saobraćaja korišćenjem kategorija u određeno vreme/dan.
Mogućnost korišćenja kategorija u blacklist modu (zabraniti sve kategorije osim označenih).
Mogućnost korišćenja izuzetaka koristeći source/destionation/domain/server/categories kao uslove.
Filtriranje saobraćaja bazirano na aplikacijama ili servisima.
Dinamičko blokiranje aplikacija u zavisnosti od rizika i indeksa produktivnosti,

Neophodne Webserver Protection funkcionalnosti

Zaštita internih web servisa i aplikacija od spoljnih napada, url hardening, sql injection zaštita, form hardening.
Provera informacija koje se šalju serveru putem web formi kako bi se sprečila zloupotreba serverskih sigurnosnih propusta.
Mogućnosti reverse proxy i dvo-faktorne korisničke autentifikacije korišćenjem prilagođene HTML forme.
Podrška za https offloading mehanizam.
Podrška za SAN sertifikate.
Dva antivirus engine-a različitih proizvođača
Podrška za cookies signing, authentification offloading basic i form authentifikacija, mogućnost podešavanja autentifikacije po serveru ili url-u.

Neophodne Email Protection funkcionalnosti

Zaštita internog mail servera, detekcija i zaustavljanje neželjenih (spam) i zaraženih poruka direktno na ulazu u mrežu.
Mogućnost enkripcije e-mail saobraćaja i zaštite od curenja informacija putem elektronske pošte (DLP). Mogućnost korisničkog upravljanja sopstvenim karantinom.
Mogućnost podešavanja po domenu (različita podešavanja za svaki domen).
Dva ili više antivirus engine-a različitih proizvođača.
Spam zaštita za SMTP, POP3 protokole, sa mogućnošću deaktiviranja spam i antivirus zaštite u zavisnosti od pošiljaoca/primaoca.

DLP (data leakage prevention) sa predefinisanim pravilima i mogućnost dodavanja sopstvenim DLP rulova koristeći regular expressions.
Kreiranje dnevnih izveštaja o blokiranim mail-ovima za svakog korisnika.
Omogućavanje korisniku da može da uradi release mail-ova i da pravi svoju black i white listu.
Integrisana podrška za enkripciju/dekripciju podrška za OpenPGP, S/MIME enkripciju.

Neophodne Wireless Protection funkcionalnosti
Centralno upravljanje bežičnim access point uređajima putem ugrađenog wireless kontrolera.
Mogućnost definisanja wireless hotspot funkcionalnosti i omogućavanje pristupa Internetu gostima putem vaučer sistema sa ograničenim vremenskim trajanjem i količinom podataka dostupnom za prenos.

Neophodne Reporting funkcionalnosti
Integrisano izveštavanje sa predefinisanim izveštajima (više od 100 predefinisanih) o hardverskim, mrežnim, web, e-mail, wireless, webserver protection i remote access statistikama i događajima.
Mogućnost definisanja eksternih servera za slanje i arhiviranje događaja i log datoteka.

Neophodne funkcionalnosti Logovanja
Mogućnost smeštanja/arhiviranja ftp serveru, SMB (CIFS), share-u ili slanje putem mail-a.
Mogućnost prosleđivanja logova na Syslog server.

Neophodne Next-generation APT funkcionalnosti
Ponuđeno rešenje mora da ima i mogućnost korišćenja cloud Sandboxing-a u cilju povećanja APT mogućnosti i što boljem i preciznijem otkrivanju zero-day napada. Sandboxing licenca treba da pokrije zaštitu Email saobraćaja i kompletnog Web saobraćaja

ПИТАЊЕ 2:
На страни 29/159 у техничкој спецификацији за Партију 9. FIREWALL, МОЛИМ Вас да одговорите за које функционалности је потребно попунити једногодишњу лиценцу,јер у многоме утиче на крајњу цену. Молим Вас да потврдите да ћете као адекватан прихватити FIREWALL уређај реномираног произвођача који захтеване функционалности постиже на адекватан начин утилизацијом својих „brand-specific" хардверских решења.

ОДГОВОР 2:

Набавља се уређај који долази са 12-то месечном Basic лиценцом, која покрива тражене firewall функционалсности.
Овај уређај је upgrade за постојеће УТМ решење које је имплементирано у ЈП ЕПС Огранак Панонске ТЕ-ТО више година уназад. Прихватиће се уређај који испуњава све захтеване функционалности из одговора 1.

Овај акт се објављује се на Порталу јавних набавки и интернет страници наручиоца.

КОМИСИЈА