SPECIFICAȚII TEHNICE

Lista de Bunuri propuse achiziționării		
	Denumirea	**Cantitatea**
B1.01.	Next Generation Firewall Tip I	20
B1.02.	Next Generation Firewall Tip II	14
B1.03.	Sistem centralizat de monitorizare și management	1

C1 - Cerințe Generale	
C1.01.	Soluția propusă trebuie să fie livrată, instalată și configurată pentru a obține o soluție complet funcțională la cheie.
C1.02.	Furnizorul va asigura executarea lucrărilor de instalarea, configurarea si migrarea serviciilor, inclusiv in afara orelor de lucru in conformitate cu planul de instalare furnizat de Beneficiar.
C1.03.	Toate componentele hardware a soluției trebuie să fie rack-mount 19”.
C1.04.	Toate componentele hardware a soluției trebuie să fie compatibile cu rețeaua de curent electric AC120/230V 50/60Hz.
C1.05.	Toate componentele hardware a soluției trebuie să aibă blocuri de alimentare interne.
C1.06.	Toate componentele hardware a soluției trebuie să fie funcționale la temperaturi de la 0°C până la 40°C.
C1.07.	Soluția propusă trebuie să fie livrată cu toate cablurile necesare pentru conectare în rack.
C1.08.	Soluția propusă trebuie să includă suport hardware și software pentru cel puțin 3 ani.
C1.09.	Soluția propusă trebuie să includă toate subscripțiile necesare pentru cel puțin 3 ani.
C1.10.	Soluția propusă trebuie să permit detectarea și filtrarea traficului după conținut (content).
C1.11.	Soluția propusă trebuie să permită detectarea și filtrarea atacurilor de tip DDoS prin definirea politicilor.
C1.12.	Soluția propusă trebuie să permită detectarea și filtrarea aplicațiilor.
C1.13.	Soluția propusă trebuie să permită stabilirea regulilor de antispam, antivirus, web filtering.

C1.14.	Soluția propusă trebuie să permită stabilirea regulilor de QoS si traffic shaping.
C1.15.	Soluția propusa trebuie sa permită stabilirea regulilor de firewall după criteriul de GeoIP.
C1.16.	Soluția propusa trebuie sa permită aplicarea regulilor de blocare a traficului de rețea având ca sursa sau destinație adresele BootNet, care se actualizează periodic.
C1.17.	Soluția propusa trebuie sa permită stabilirea regulilor de filtrare web – web inspection/Filter.
C1.18.	Soluția propusă trebuie să permită divizarea logica, prin atribuirea resurselor limita, ce va permite furnizarea pentru fiecare unitate logica cel puțin următoarea funcționalități: • Gestionarea Tabelei de Rutare • Gestionarea Tabelei de NAT • Gestionarea Tabelei Firewall • Gestionarea VPN Instance • Gestionarea Politicilor de securitate(Application,WebFilter,etc) • Gestionarea Interfețelor fizice si logice atribuite • Etc.
C1.19.	Soluția propusa trebuie sa asigure cerințele minime pentru asigurarea disponibilității înalte: • Functionare Active-Active, Active-Passive • Functionalitate Stateful Failover (Firewall si VPN) • Detectare si notificare pentru echipament nefunctional • Monitorizarea conexiunii la retea • Functionalitate Link Failover
C1.20.	Soluția propusa trebuie sa asigure cerințele minime pentru asigurarea monitorizării componentelor hardware: • Monitorizare grafica in timp real si istorica • Optiune de pastrare a log-urilor pe spatiu de stocare cloud-based oferit de producator • Suport syslog • Suport SNMP v1/v2c/v3 • Notificare prin e-mail pentru alerte • Suport sFlow si Netflow

C2 – Cerințe funcționale Next Generation Firewall Tip I	
C2.01.	Soluția propusă trebuie să permită filtrarea traficului de cel puțin 20Gbps.
C2.02.	Soluția propusă trebuie să aibă capacitatea de tunelare IPSec(VPN) de cel puțin 5 Gbps.
C2.03.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului SSL de cel puțin 800Mbps.
C2.04.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului prin activarea funcționalului de IPS de cel puțin 2Gbps.
C2.05.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni simultane TCP până la 2 milioane.
C2.06.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni noi de cel puțin 120 000 pe secunda.
C2.07.	Fiecare echipament hardware trebuie să conțină cel puțin 4 sloturi 1xGE SFP, cu SFP module incluse.
C2.08.	Fiecare echipament hardware trebuie să conțină cel puțin 12 porturi 1xGE RJ45.
C2.09.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Management Port.
C2.10.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Console Port.

C3 – Cerințe funcționale Next Generation Firewall Tip II	
C3.01.	Soluția propusă trebuie să permite filtrarea traficului de pînă la 30Gbps.
C3.02.	Soluția propusă trebuie să aibă capacitatea de tunelare IPSec de pînă la 20Gbps.
C3.03.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului SSL de pînă la 5Gbps.
C3.04.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului prin activarea funcționalului de IPS de cel puțin 5Gbps.
C3.05.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni simultane TCP pînă la 8 milioane.
C3.06.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni noi de cel puțin 300 000 pe secunda.
C3.07.	Fiecare echipament hardware trebuie să conțină cel puțin 2 sloturi 10xGE SFP+, cu modulele SFP+ incluse.
C3.08.	Fiecare echipament hardware trebuie să conțină cel puțin 8 sloturi 1GE SFP, cu cel puțin 4 SFP module incluse.
C3.09.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Management Port.
C3.10.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Console Port.

C4 - Cerințe funcționale - Sistem centralizat de monitorizare și management	
C4.01.	Sistemul propus trebuie să permită aplicarea politicilor de filtrare centralizat pentru toate componentele.
C4.02.	Sistemul propus trebuie să reprezinte un singur punct de comandă, control, analiză și raportare, furnizata de același vendor ca si echipamentele.
C4.03.	Sistemul trebuie sa fie capabil sa gestioneze toate componentele livrate(NGFW Tip I si TIP II).
C4.04.	Sistemul trebuie sa fie capabil sa gestioneze cel puțin 250 de echipamente prin extinderea licenței, daca aceasta prevede.
C4.05.	Sistemul propus trebuie să permită adăugarea unui component hardware nou fără a fi configurat din start cu aplicarea lui unor anumite politici.
C4.06.	Sistemul propus trebuie să permită rapoarte pe utilizarea rețelei și capacitate.
C4.07.	Sistemul propus trebuie să permită crearea regulilor de avertizare granulare cu raportarea personalului cheie.
C4.08.	Soluția trebuie să permită crearea profilurilor individuale pentru inspecția SSL în funcție de cerințele politicii.
C4.09.	Sistemul trebuie să permită utilizarea certificatului de autoritate de certificare (CA) pentru a decripta traficul criptat prin Secure Sockets Layer (SSL).
C4.10.	Sistemul trebuie să permită configurarea protocoalelor SSL care vor fi inspectate.
C4.11.	Sistemul trebuie să permită configurarea porturilor care vor fi asociate cu protocoalele SSL în scopul inspecției.
C4.12.	Sistemul trebuie să permită configurarea site-urilor care vor fi scutite de inspecția SSL.
C4.13.	Sistemul trebuie să permită configurarea restricțiilor pentru certificatele SSL nevalide.
C4.14.	Sistemul trebuie să permită reguli pentru inspectarea traficului SSH (Secure Shell).
C4.15.	Sistemul va furniza cel puțin următoarele funcționalități generale: • Administrare prin WEB UI (HTTP/HTTPS), Telnet, Secure Command Shell (SSH), Command Line Interface (CLI) • Administrare bazata pe profile • Posibilitatea de a utiliza autentificare administrativa prin doi factori • Comunicare criptata si autentificare cu echipamentele administrate • Alertare prin e-mail • Alertare prin SNMP • Alertare prin Syslog • Configurare setări de bază sistem • Suport din interfața grafica de tip „online help” • Gestiune a echipamentelor administrate: adăugare, modificare, ștergere • Vizualizare informații sistem/resurse • Vizualizare perioada valabilitate licențe cu alertare prealabila expirării acestora • Vizualizare statistici funcționare echipament din punct de vedere hardware • Funcționalitate de export/import a configurației

	• Opțiune de încărcare a configurației din fabrica • Opțiune de formatare discurilor HDD • Opțiune upgrade firmware • Posibilitatea de configurare prin API (JSON, XML)
C4.16.	Sistemul trebuie sa ofere cel puțin următoarele funcționalități de gestionare centralizata a echipamentelor: • Posibilitatea alocării echipamentelor administrate in domenii administrative • Acces administrativ separat pentru domeniile administrative • Distribuirea pe baza de profile a politicilor de securitate pentru echipamentele administrate • Posibilitatea grupării echipamentelor administrare in scopul administrării pe grupuri de echipamente • Posibilitatea reutilizării obiectelor definite local in cadrul mai multor profile de configurații • Posibilitatea realizării de audit in vederea verificării configurațiilor de securitate a echipamentelor administrate • Posibilitatea de a efectua modificări in configurațiile echipamentelor gestionate si de aplicarea a acestora doar cu aprobarea unui administrator cu drepturi superioare celui care a efectuat modificările in configurații • Posibilitatea de a păstră configurațiile echipamentelor administrate sub forma de revizii cronologice, cu posibilitatea vizualizării diferențelor intre revizii diferite ale configurației • Posibilitatea de funcționare ca server de actualizare a semnăturilor utilizate de serviciile de securitate ce rulează pe echipamentele administrate • Monitorizarea in timp real a echipamentelor administrate • Posibilitatea rulării de scripturi(comenzi CLI si TCL) in scopul configurării echipamentelor administrate • Posibilitatea de agregare a ligurilor trimise de echipamentele administrate • Posibilitatea vizualizării a logurilor colectate per echipament administrat • Posibilitatea de realizare de grafice de tip „drill down” pe baza logurilor colectate de la echipamentele administrate • Posibilitatea de generare de rapoarte personalizate pe baza logurilor colectate de la echipamentele administrate • Posibilitatea de programare in timp a schimbarii configuratiei echipamentelor administrate si a generării rapoartelor