Specificații tehnice

Anexa 1

Lista de Bunuri propuse achiziționării		
	Denumirea	**Cantitatea**
B1.01.	Next Generation Firewall Tip I	25
B1.02.	Next Generation Firewall Tip II	30
B1.03.	Next Generation Firewall Tip III	14
B1.04.	Sistem de asigurare a securității serviciului de poștă electronică	2
B1.05.	Sistem centralizat de monitorizare și management	1

C1	Cerințe Generale
C1.01.	Soluția livrată trebuie sa fie funcțională si sa corespunda tuturor cerințelor, fără careva limitări.
C1.02.	Furnizorul va asigura executarea activitatilor de instalare, configurare si migrare a serviciilor, inclusiv in afara orelor de lucru.
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	
C3.01.	Soluția propusă trebuie să permită filtrarea traficului de cel puțin 4Gbps.
C3.02.	Soluția propusă trebuie să aibă capacitatea de tunelare IPSec(VPN) de cel puțin 3 Gbps.

C3.03.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului SSL de cel puțin 200Mbps.
C3.04.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului prin activarea funcționalului de IPS de cel puțin 500Mbps.
C3.05.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni simultane TCP până la 2 milioane.
C3.06.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni noi de cel puțin 30 000 pe secunda.
C3.07.	Fiecare echipament hardware trebuie să conțină cel puțin 2 sloturi 1xGE SFP , cu SFP module incluse.
C3.08.	Fiecare echipament hardware trebuie să conțină cel puțin 12 porturi 1xGE RJ45.
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.

C3 – Cerințe funcționale Next Generation Firewall Tip I I	
C3.01.	Soluția propusă trebuie să permită filtrarea traficului de cel puțin 20Gbps.
C3.02.	Soluția propusă trebuie să aibă capacitatea de tunelare IPSec(VPN) de cel puțin 5 Gbps.
C3.03.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului SSL de cel puțin 800Mbps.
C3.04.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului prin activarea funcționalului de IPS de cel puțin 2Gbps.
C3.05.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni simultane TCP până la 2 milioane.
C3.06.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni noi de cel puțin 120 000 pe secunda.
C3.07.	Fiecare echipament hardware trebuie să conțină cel puțin 4 sloturi 1xGE SFP, cu SFP module incluse.
C3.08.	Fiecare echipament hardware trebuie să conțină cel puțin 12 porturi 1xGE RJ45.
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 Next Generation Firewall Tip III	
C4.01.	Soluția propusă trebuie să permite filtrarea traficului de pînă la 30Gbps.
C4.02.	Soluția propusă trebuie să aibă capacitatea de tunelare IPSec de pînă la 20Gbps.
C4.03.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului SSL de pînă la 5Gbps.
C4.04.	Soluția propusă trebuie să aibă capacitatea de inspectare a traficului prin activarea funcționalului de IPS de cel puțin 5Gbps.
C4.05.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni simultane TCP pînă la 8 milioane.
C4.06.	Soluția propusă trebuie să aibă capacitatea de a stabili sesiuni noi de cel puțin 300 000 pe secunda.
C4.07.	Fiecare echipament hardware trebuie să conțină cel puțin 2 sloturi 10xGE SFP+, cu modulele SFP+ incluse.
C4.08.	Fiecare echipament hardware trebuie să conțină cel puțin 8 sloturi 1GE SFP, cu cel puțin 4 SFP module incluse.
C4.09.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Management Port.
C4.10.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Console Port.

C5 Cerințe funcționale - Sistem de asigurare a securității serviciului de poștă electronică	
C5.01.	Sistemul propus trebuie să fie compatibil cu medii virtualizate bazate pe tehnologia VMware vSphere.
C5.02.	Sistemul propus trebuie să asigure funcționalitate de protecție a serviciului de poștă electronică, în timp real, contra cel puțin următoarelor tipuri de atacuri; - Spam; - Spoofing; - Phishing; - Fraud; - Virus; - Malware; - Zero Day / Zero Hour.
C5.03.	Soluția trebuie sa ofere o interfața unica de tip web pentru configurarea, gestionarea și administrarea soluției, precum si/sau utilizând sistemul centralizat de monitorizare și management.
C5.04.	Accesul la consola de administrare trebuie să fie permisă doar în baza de protocoale securizate.
C5.05.	Soluția trebuie să permită o configurare granulară de roluri, atât cu permisiuni

	administrative, cât și cu permisiuni limitate.
C5.06.	Soluția trebuie să ofere instrumente de analiză/depanare a configurărilor, incidentelor (troubleshooting) direct din interfața unică de administrare.
C5.07.	Soluția trebuie să ofere instrumente suplimentare (avansate) de de analiză/depanare a configurărilor, incidentelor (troubleshooting) prin acces direct la sistemul de operare.
C5.08.	Soluția trebuie să asigure funcționalitate stabilă la o capacitate de minimă de: - 15000 conturi; - 300 de domenii; - 200000 mesaje / oră (fără a lua în calcul volumul de mesaje aflate în coadă)..
C5.09.	Soluția trebuie să permită configurarea multiplelor adrese IP pentru traficul de serviciu(IN/OUT).
C5.10.	Soluția trebuie să permită asignarea adreselor IP dedicate per domeniu poștal.
C5.11.	Soluția trebuie să posede mecanisme native de funcționare în regim de înaltă disponibilitate (HA) sau balansare (LB), asigurând cel puțin următoarele funcționalități: - Sincronizare configurări; - Sincronizare înregistrări de audit (SMTP de intrare/ieșire, de sistem, etc); - Sincronizarea cozii de mesaje; - etc
C5.12.	Soluția trebuie să permită vizualizarea înregistrărilor de audit STMP de intrare și ieșire, cu posibilități avansate de filtrate a acestora, cel puțin în bază de destinatar, sender, conținut, domeniu, tipul acțiunii, perioadă.
C5.13.	Sistemul trebuie să permită retenția mesajelor în coada de așteptare, cît și gestionarea cozii de mesaje
C5.14.	Sistemul trebuie să permită gestionarea din interfața unică pentru cel puțin următoarele funcționalități: - Blocarea mesajelor de intrare/ieșire per adresă IP și domeniu; - Limitare bazată pe rata de transmitere a mesajelor; - Whitelist / Blacklist în bază de domeniu și cont poștal; - Limitare/Blocare/Marcare în bază de tip de atașament și conținutul acestuia; - Limitare/Blocare/Marcare în baza de subiect și conținut al mesajului
C5.15.	Sistemul trebuie să permită livrarea forțată a mesajelor
C5.16.	Sistemul trebuie să permită retransmiterea înregistrărilor de audit în baza protocolului syslog
C5.17.	Sistemul trebuie să posede mecanisme native de gestionare a copiilor de rezervă aferente configurărilor soluției și posibilitatea de restabilire a acestora
C5.18.	Sistemul trebuie să posede un mecanism propriu de monitorizare a stării: - parametri fizici (CPU, RAM, Storage); - Numărul de mesaje în coada de intrare/ieșire;
C5.19.	Sistemul trebuie să conțină un mecanism de alertare nativ prin SMTP
C5.20.	Sistemul trebuie să permită configurarea și generarea de rapoarte, inclusiv livrarea acestora pe e-mail.

C6 Cerințe funcționale - Sistem centralizat de monitorizare și management	
C6.01.	Sistemul propus trebuie să permită aplicarea politicilor de filtrare centralizat pentru toate componentele.
C6.02.	Sistemul propus trebuie să reprezinte un singur punct de comandă, control, analiză și raportare, furnizata de același vendor ca si echipamentele.
C6.03.	Sistemul trebuie sa fie capabil sa gestioneze toate componentele livrate(NGFW Tip I, TIP II și TIP III).
C6.04.	Sistemul trebuie sa fie capabil sa gestioneze cel puțin 330 de echipamente, si/sau echipamente logice(virtuale), prin extinderea licenței, daca aceasta prevede.
C6.05.	Sistemul propus trebuie să permită adăugarea unui component hardware nou fără a fi configurat din start cu aplicarea lui unor anumite politici.
C6.06.	Sistemul propus trebuie să permită rapoarte pe utilizarea rețelei și capacitate.
C6.07.	Sistemul propus trebuie să permită crearea regulilor de avertizare granulare cu raportarea personalului cheie.
C6.08.	Soluția trebuie să permită crearea profilurilor individuale pentru inspecția SSL în funcție de cerințele politicii.
C6.09.	Sistemul trebuie să permită utilizarea certificatului de autoritate de certificare (CA) pentru a decripta traficul criptat prin Secure Sockets Layer (SSL).
C6.10.	Sistemul trebuie să permită configurarea protocoalelor SSL care vor fi inspectate.
C6.11.	Sistemul trebuie să permită configurarea porturilor care vor fi asociate cu protocoalele SSL în scopul inspecției.
C6.12.	Sistemul trebuie să permită configurarea site-urilor care vor fi scutite de inspecția SSL.
C6.13.	Sistemul trebuie să permită configurarea restricțiilor pentru certificatele SSL nevalide.
C6.14.	Sistemul trebuie să permită reguli pentru inspectarea traficului SSH (Secure Shell).
C6.15.	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)
C6.16.	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

Anexa 2

Lista de Bunuri propuse achiziționării		
	Denumirea	**Cantitatea**
B1.01.	Echipamente Telecomunicaționale Tip I	5
B1.02.	Echipamente Telecomunicaționale Tip II	10

C1 Cerințe funcționale Echipamente Telecomunicaționale TIP-I	
C1.01.	Echipamentele trebuie să aibă cel puțin 48 porturi SFP+ și 4 porturi 40 Gigabit QSFP+ (Uplink)
C1.02.	Echipamentele trebuie să fie rack-mount 19”
C1.03.	Echipamentele trebuie să fie compatibile cu rețeaua de curent electric AC120/230V 50/60Hz.
C1.04.	Echipamentele trebuie să susțină cel puțin 32000 MAC adrese
C1.05.	Echipamentele trebuie să susțină Jumbo Frame de 9000 bytes
C1.06.	Echipamentele trebuie să susțină cel puțțin 1200 Gbps capacitate de switching
C1.07.	Echipamentele trebuie să susțină autentificarea prin Radius, TACACS, Secure Shell (SSH), Kerberos
C1.08.	Echipamentele trebuie să susțină 802.1x autentificare, ARP inspection, ACL, BPDU, CoPP, DHCP Snooping, Link Aggregation Control Protocol (LACP), Remote Switch Port Analyzer (RSPAN), Uni-Directional Link Detection (UDLD), Virtual Route Forwarding-Lite (VRF-Lite)
C1.09.	Echipamentele trebuie să susțină configurarea prin CLI, NETCONF, RESTCONF, RMON 1, RMON 2, SNMP 1, SNMP 2c, SNMP 3
C1.10.	Echipamentele trebuie să susțină Flow export pe bază de ipv4 source address, destination address, ipv4 protocol, source-port, destination-port, L2-vlan
C1.11.	Echipamentele trebuie să susțină rutarea statică
C1.12.	Echipamentele trebuie să aibă cel puțin 1 RJ-45 Console port
C1.13.	Echipamentele trebuie să aibă cel pțin 1 RJ-45 Management port

C2 Cerințe funcționale Echipamente Telecomunicaționale TIP-II	
C2.01.	Echipamentele trebuie să aibă cel puțin 24 porturi 10/100/1000 RJ45 și 4 porturi 10 Gigabit SFP+ (Uplink)
C2.02.	Echipamentele trebuie să fie rack-mount 19”
C2.03.	Echipamentele trebuie să fie compatibile cu rețeaua de curent electric AC120/230V 50/60Hz.
C2.04.	Echipamentele trebuie să susțină cel puțin 32000 MAC adrese
C2.05.	Echipamentele trebuie să susțină Jumbo Frame de 9000 bytes
C2.06.	Echipamentele trebuie să susțină cel puțțin 208Gbps capacitate de switching
C2.07.	Echipamentele trebuie să susțină autentificarea prin Radius, TACACS, Secure Shell (SSH), Kerberos
C2.08.	Echipamentele trebuie să susțină 802.1x autentificare, ARP inspection, ACL, BPDU, CoPP, DHCP Snooping, Link Aggregation Control Protocol (LACP), Remote Switch Port Analyzer (RSPAN), Uni-Directional Link Detection (UDLD), Virtual Route Forwarding-Lite (VRF-Lite)
C2.09.	Echipamentele trebuie să susțină configurarea prin CLI, NETCONF, RESTCONF, RMON 1, RMON 2, SNMP 1, SNMP 2c, SNMP 3
C2.10.	Echipamentele trebuie să susțină Flow export pe bază de ipv4 source address, destination address, ipv4 protocol, source-port, destination-port, L2-vlan
C2.11.	Echipamentele trebuie să susțină rutarea statică
C2.12.	Echipamentele trebuie să aibă cel puțin 1 RJ-45 Console port
C2.13.	Echipamentele trebuie să aibă cel pțin 1 RJ-45 Management port