Caietul de sarcini

Obiectul: **Echipamente (NGFW-uri)**

Autoritatea contractantă: **I.P. Serviciul Tehnologia Informației și Securitate Cibernetică**

Lista de Bunuri propuse achiziționării		
	Denumirea	**Cantitatea**
B1.01.	NGFW Tip I	50
B1.02.	NGFW Tip II	25
B1.03.	NGFW Tip III	28

H1	**Cerințe Hardware NGFW Tip I**
H1.01.	Echipamentul trebuie să fie 1U rack-mount 19” sau versiunea compactă dotat kit de instalare in rack
H1.02.	Echipamentul trebuie să aibă cel puțin 8 porturi RJ45 10/100/1000 Mbps
H1.03.	Echipamentul trebuie să aibă cel puțin 2 porturi optice SFP+ (10Gbps)
H1.04.	Echipamentul trebuie să aibă și consolă
H1.05.	Echipamentul trebuie să fie dotat cu 2 surse de alimentare redundante
H1.06.	Echipamentul trebuie să fie compatibile cu rețeaua de curent electric AC220V AC 50/60Hz.
H1.07.	Echipamentul ofertat trebuie să suporte configurarea în regim de Disponibilitate Sporită (High Availability - HA), respectând următoarele cerințe minime: - Moduri de operare: Trebuie să permită funcționarea atât în mod Active-Passive (pentru redundanță totală), cât și în mod Active-Active (pentru distribuția sarcinii/load balancing), prin interconectarea cu un al doilea echipament identic.

	- Sincronizarea datelor: Sistemul trebuie să asigure sincronizarea automată și în timp real a configurațiilor, tabelelor de sesiuni (session state), politicilor de securitate și a bazelor de date de semnături între cele două unități din cluster. - Timp de comutare (Failover): În cazul defectării unității principale sau a pierderii conectivității pe un port monitorizat, comutarea traficului către unitatea secundară trebuie să se realizeze automat, sub o secundă (sub-second failover), fără a întrerupe sesiunile active de utilizator (stateful failover). - Monitorizarea legăturilor (Interface Monitoring): Posibilitatea de a monitoriza starea link-urilor critice (WAN/LAN); în cazul în care un link pică pe unitatea activă, clusterul trebuie să transfere automat rolul de "Master" către unitatea care are link-urile funcționale. - Management Unificat: Administrarea clusterului de tip HA trebuie să se facă printr-o singură adresă IP de management, indiferent de unitatea care este activă în acel moment.Actualizări fără întrerupere (Non-Disruptive Upgrade): Suport pentru actualizarea firmware-ului în cadrul clusterului fără a cauza perioade de indisponibilitate a serviciilor (rolling upgrade).
H1.08.	Echipamentul trebuie să poată asigura Firewall minim 20 Gbps (pentru pachete de 1518 bytes)
H1.09.	Echipamentul trebuie să poată asigura Threat Protection minim 2 Gbps cu modulul de Intrusiuni , Antivirus și Control Aplicație activat
H1.010.	Echipamentul trebuie să poată asigura criptare IPsec minim 20 Gbps
H1.011.	Echipamentul trebuie să poată asigura minim 2M (milion) de sesiuni TCP concurente
H1.012.	Echipamentul trebuie să poată asigura minim 100000 sesiuni noi/secundă
H1.013.	Echipamentul trebuie să asigure un throughput pentru inspecția traficului criptat (SSL Inspection/Deep Packet Inspection) de minim 2 Gbps, cu suport obligatoriu pentru protocolul TLS 1.3.
H1.014.	Echipamentul trebuie să poată asigura direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).
H1.015.	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.

C1	**Cerințe funcționale NGFW TIP-I**
C1.01.	Echipamentele trebuie să susțină IEEE 802.1Q VLAN.

C1.02.	Agregare: Suport pentru IEEE 802.3ad (LACP) cu capacitatea de a grupa până la 4 porturi de 1G/10G într-un singur canal logic
C1.03.	Echipamentele trebuie să susțină Autentificare prin RADIUS, TACACS+, SSH v2, SNMP v3 și suport pentru Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS
C1.04.	Echipamentul trebuie să suporte protocoalele de tunelare cum ar fi : - GRE - IPIP - L2TP - VxLAN
C1.05.	Echipamentul trebuie să suporte nativ capabilități de Zero Trust Network Access (ZTNA) pentru verificarea identității utilizatorului și a stării dispozitivului la fiecare încercare de conectare, indiferent de locația acestuia
C1.06.	Echipamentul trebuie sa aibă posibilitatea de a partaja informații despre amenințări cu alte elemente de rețea (switch-uri, access point-uri, endpoint-uri) de la același producător sau prin API-uri deschise, pentru un răspuns automatizat la incidente.
C1.07.	Echipamentul trebuie să includă o interfață grafică (GUI) intuitivă care să permită vizualizarea în timp real a topologiei de rețea, a aplicațiilor utilizate (Application Control)
C1.08.	Echipamentul trebuie să suporte "Forward Error Correction" (FEC) și "Packet Duplication" pentru a asigura calitatea aplicațiilor critice (VoIP, Video) pe legături WAN instabile
C1.09.	Echipamentul trebuie să suporte protocoale de rutare dinamică bazate pe standarde deschise (IETF), incluzând minimum: RIPv2/ng, OSPFv2/v3, IS-IS și BGPv4 (iBGP/eBGP), atât pentru IPv4 cât și pentru IPv6, rutarea bazată pe politici (Policy-Based Routing - PBR) și rutarea multicast (PIM-SM/DM)
C1.010.	Echipamentul trebuie să suporte Data Leak Prevention (DLP)
C1.011.	Echipamentul trebuie să suporte segmentarea virtuală în cel puțin 10 instanțe logice/virtuale independente (ex: VDOM, Contexts, Virtual Systems sau echivalent), pentru a permite izolarea completă a traficului între diferite departamente sau entități
C1.012.	La expirarea licențelor de securitate, echipamentul trebuie să își păstreze funcționalitatea de bază (Firewall, Routing, VPN, SD-WAN, interfață de management) fără limitarea numărului de utilizatori sau a lățimii de bandă

H2	**Cerințe Hardware NGFW Tip II**
H2.01.	Echipamentul trebuie să fie 1U rack-mount 19” și de adâncimea maximă de 500mm
H2.02.	Echipamentul trebuie să aibă cel puțin 12 porturi RJ45 10/100/1000 Mbps
H2.03.	Echipamentul trebuie să aibă cel puțin 4 porturi optice SFP+ (10Gbps)

H2.04.	Echipamentul trebuie să aibă cel puțin 8 porturi optice SFP (1Gbps)
H2.05.	Echipamentul trebuie să fie dotat cu 2 surse de alimentare redundante
H2.06.	Echipamentul trebuie să fie compatibile cu rețeaua de curent electric AC220V AC 50/60Hz.
H2.07.	Echipamentul ofertat trebuie să suporte configurarea în regim de Disponibilitate Sporită (High Availability - HA), respectând următoarele cerințe minime: - Moduri de operare: Trebuie să permită funcționarea atât în mod Active-Passive (pentru redundanță totală), cât și în mod Active-Active (pentru distribuția sarcinii/load balancing), prin interconectarea cu un al doilea echipament identic. - Sincronizarea datelor: Sistemul trebuie să asigure sincronizarea automată și în timp real a configurațiilor, tabelelor de sesiuni (session state), politicilor de securitate și a bazelor de date de semnături între cele două unități din cluster. - Timp de comutare (Failover): În cazul defectării unității principale sau a pierderii conectivității pe un port monitorizat, comutarea traficului către unitatea secundară trebuie să se realizeze automat, sub o secundă (sub-second failover), fără a întrerupe sesiunile active de utilizator (stateful failover). - Porturi dedicate High Availability: Echipamentul trebuie să dispună de interfețe fizice dedicate pentru legătura de tip "Heartbeat" și sincronizarea datelor, pentru a nu consuma din lățimea de bandă a porturilor de date. - Monitorizarea legăturilor (Interface Monitoring): Posibilitatea de a monitoriza starea link-urilor critice (WAN/LAN); în cazul în care un link pică pe unitatea activă, clusterul trebuie să transfere automat rolul de "Master" către unitatea care are link-urile funcționale. - Management Unificat: Administrarea clusterului de tip HA trebuie să se facă printr-o singură adresă IP de management, indiferent de unitatea care este activă în acel moment.Actualizări fără întrerupere (Non-Disruptive Upgrade): Suport pentru actualizarea firmware-ului în cadrul clusterului fără a cauza perioade de indisponibilitate a serviciilor (rolling upgrade).
H2.08.	Echipamentul trebuie să asigure o latență ultra-scăzută de maxim 10 microsecunde în regim de firewall.
H2.09.	Echipamentul trebuie să poată asigura Firewall minim 25 Gbps
H2.010.	Echipamentul trebuie să poată asigura Threat Protection minim 2.5 Gbps cu modulul de Intrusiuni , Antivirus și Control Aplicație activat

H2.011.	Echipamentul trebuie să poată protecție NGFW minim 3 Gbps
H2.012.	Echipamentul trebuie să poată asigura criptare IPsec minim 25 Gbps
H2.013.	Echipamentul trebuie să poată asigura minim 2M (milioane) de sesiuni TCP concurente
H2.014.	Echipamentul trebuie să poată asigura minim 120000 sesiuni noi/secundă
H2.015.	Echipamentul trebuie să poată asigura inspecția SSL minim 3 Gbps
H2.016.	Echipamentul trebuie să asigura capacitatea de a inspecta traficul criptat (HTTPS/SSL/TLS 1.3) fără degradarea critică a performanțe
H2.017.	Echipamentul trebuie să poată asigura direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).
H2.018.	Echipamentul trebuie să poată actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS
H2.019.	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.

C2	**Cerințe funcționale NGFW TIP-II**
C2.01.	Echipamentele trebuie să susțină IEEE 802.1Q VLAN.
C2.02.	Agregare: Suport pentru IEEE 802.3ad (LACP) cu capacitatea de a grupa până la 8 porturi de 1G/10G într-un singur canal logic
C2.03.	Echipamentele trebuie să susțină Autentificare prin RADIUS, TACACS+, SSH v2, SNMP v3 și suport pentru Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS
C2.04.	Echipamentul trebuie să suporte protocoalele de tunelare cum ar fi : - GRE - IPIP - L2TP - VxLAN
C2.05.	Funcționalitatea ZTNA (Zero Trust Network Access) trebuie să fie nativă în sistemul de operare, permițând aplicarea politicilor de acces bazate pe identitate fără a necesita licențiere sau mașini virtuale suplimentare pentru funcțiile de bază (ZTNA Tags/Access Proxy).
C2.06.	Echipamentul trebuie sa aibă posibilitatea de a partaja informații despre amenințări cu alte elemente de rețea (switch-uri, access point-uri, endpoint-uri) de la același producător sau prin API-uri deschise, pentru un răspuns automatizat la incidente.

C2.07.	Echipamentul trebuie să includă o interfață grafică (GUI) intuitivă care să permită vizualizarea în timp real a topologiei de rețea, a aplicațiilor utilizate (Application Control)
C2.08.	Echipamentul trebuie să suporte "Forward Error Correction" (FEC) și "Packet Duplication" pentru a asigura calitatea aplicațiilor critice (VoIP, Video) pe legături WAN instabile
C2.09.	Echipamentul trebuie să suporte protocoale de rutare dinamică bazate pe standarde deschise (IETF), incluzând minimum: RIPv2/ng, OSPFv2/v3, IS-IS și BGPv4 (iBGP/eBGP), atât pentru IPv4 cât și pentru IPv6, rutarea bazată pe politici (Policy-Based Routing - PBR) și rutarea multicast (PIM-SM/DM)
C2.010.	Echipamentul trebuie să suporte Data Leak Prevention (DLP)
C2.011.	Echipamentul trebuie să suporte segmentarea virtuală în cel puțin 10 instanțe logice independente (Virtual Domains / VDOMs sau echivalent), pentru a permite izolarea completă a traficului între diferite departamente sau entități
C2.012.	Funcționalul echipamentului nu trebuie să fie afectat la expirarea suportului de la producător cu excepția actualizărilor de securitate

H3	**Cerințe Hardware NGFW Tip III**
H3.01.	Echipamentul trebuie să fie 1U rack-mount 19” și de adâncimea maximă de 500mm
H3.02.	Echipamentul trebuie să aibă cel puțin 12 porturi RJ45 10/100/1000 Mbps
H3.03.	Echipamentul trebuie să aibă cel puțin 4 porturi optice SFP+ (10Gbps)
H3.04.	Echipamentul trebuie să aibă cel puțin 8 porturi optice SFP (1Gbps)
H3.05.	Echipamentul trebuie să fie dotat cu 2 surse de alimentare
H3.06.	Echipamentul trebuie să fie compatibile cu rețeaua de curent electric 220V AC 50/60Hz.
H3.07.	Echipamentul ofertat trebuie să suporte configurarea în regim de Disponibilitate Sporită (High Availability - HA), respectând următoarele cerințe minime: - Moduri de operare: Trebuie să permită funcționarea atât în mod Active-Passive (pentru redundanță totală), cât și în mod Active-Active (pentru distribuția sarcinii/load balancing), prin interconectarea cu un al doilea echipament identic. - Sincronizarea datelor: Sistemul trebuie să asigure sincronizarea automată și în timp real a configurațiilor, tabelelor de sesiuni (session state), politicilor de securitate și a bazelor de date de semnături între cele două unități din cluster.

	- Timp de comutare (Failover): În cazul defectării unității principale sau a pierderii conectivității pe un port monitorizat, comutarea traficului către unitatea secundară trebuie să se realizeze automat, sub o secundă (sub-second failover), fără a întrerupe sesiunile active de utilizator (stateful failover). - Porturi dedicate High Availability: Echipamentul trebuie să dispună de interfețe fizice dedicate pentru legătura de tip "Heartbeat" și sincronizarea datelor, pentru a nu consuma din lățimea de bandă a porturilor de date. - Monitorizarea legăturilor (Interface Monitoring): Posibilitatea de a monitoriza starea link-urilor critice (WAN/LAN); în cazul în care un link pică pe unitatea activă, clusterul trebuie să transfere automat rolul de "Master" către unitatea care are link-urile funcționale. - Management Unificat: Administrarea clusterului de tip HA trebuie să se facă printr-o singură adresă IP de management, indiferent de unitatea care este activă în acel moment.Actualizări fără întrerupere (Non-Disruptive Upgrade): Suport pentru actualizarea firmware-ului în cadrul clusterului fără a cauza perioade de indisponibilitate a serviciilor (rolling upgrade).
H3.08.	Echipamentul trebuie să asigure o latență ultra-scăzută de maxim 10 microsecunde în regim de firewall.
H3.09.	Echipamentul trebuie să poată asigura Firewall minim 35 Gbps
H3.010.	Echipamentul trebuie să poată asigura Threat Protection minim 6 Gbps cu modulul de Intrusiuni , Antivirus și Control Aplicație activat
H3.011.	Echipamentul trebuie să poată protecție NGFW minim 6 Gbps
H3.012.	Echipamentul trebuie să poată asigura criptare IPsec minim 35 Gbps
H3.013.	Echipamentul trebuie să poată asigura minim 5M (milioane) de sesiuni TCP concurente
H3.014.	Echipamentul trebuie să poată asigura minim 200000 sesiuni noi/secundă
H3.015.	Echipamentul trebuie să asigure un throughput pentru inspecția traficului criptat (SSL Inspection/Deep Inspection) de minim 6 Gbps, cu suport obligatoriu pentru protocolul TLS 1.3.
H3.016.	Echipamentul trebuie să poată asigura direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).
H3.017.	Echipamentul trebuie să poată actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS

H3.018.	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.

C3	Cerințe funcționale NGFW TIP-III
C3.01.	Echipamentele trebuie să susțină IEEE 802.1Q VLAN.
C3.02.	Agregare: Suport pentru IEEE 802.3ad (LACP) cu capacitatea de a grupa până la 8 porturi de 1G/10G într-un singur canal logic
C3.03.	Echipamentele trebuie să susțină Autentificare prin RADIUS, TACACS+, SSH v2, SNMP v3 și suport pentru Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS
C3.04.	Echipamentul trebuie să suporte protocoalele de tunelare cum ar fi : - GRE - IPIP - L2TP - VxLAN
C3.05.	Echipamentul trebuie să suporte nativ capabilități de Zero Trust Network Access (ZTNA) pentru verificarea identității utilizatorului și a stării dispozitivului la fiecare încercare de conectare, indiferent de locația acestuia
C3.06.	Echipamentul trebuie sa aibă posibilitatea de a partaja informații despre amenințări cu alte elemente de rețea (switch-uri, access point-uri, endpoint-uri) de la același producător sau prin API-uri deschise, pentru un răspuns automatizat la incidente.
C3.07.	Echipamentul trebuie să includă o interfață grafică (GUI) intuitivă care să permită vizualizarea în timp real a topologiei de rețea, a aplicațiilor utilizate (Application Control)
C3.08.	Echipamentul trebuie să suporte "Forward Error Correction" (FEC) și "Packet Duplication" pentru a asigura calitatea aplicațiilor critice (VoIP, Video) pe legături WAN instabile
C3.09.	Echipamentul trebuie să suporte protocoale de rutare dinamică bazate pe standarde deschise (IETF), incluzând minimum: RIPv2/ng, OSPFv2/v3, IS-IS și BGPv4 (iBGP/eBGP), atât pentru IPv4 cât și pentru IPv6, rutarea bazată pe politici (Policy-Based Routing - PBR) și rutarea multicast (PIM-SM/DM)
C3.010.	Echipamentul trebuie să suporte Data Leak Prevention (DLP)
C3.011.	Echipamentul trebuie să suporte segmentarea virtuală în cel puțin 10 instanțe logice independente (Virtual Domains / VDOMs sau echivalent), pentru a permite izolarea completă a traficului între diferite departamente sau entități
C3.012.	Funcționalitatea de bază a echipamentului (rutare, firewall, VPN) nu trebuie să fie condiționată sau blocată la expirarea abonamentelor de suport/securitate (cu excepția actualizărilor de semnături)