I.P. SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ (STISC)

TABELA DE CONFORMITATE — Achiziție echipamente NGFW (STAAP)

Ofertantul completează coloanele „Conformitate", „Produsul / modelul ofertat" și „Justificare / referință" pentru fiecare poziție. Toate cerințele sunt minime și obligatorii.

Cod cerință	Cerință tehnică minimă obligatorie	Produsul / modelul ofertat	Conformitate (Conform / Neconform)	Justificare / referință (datasheet, pagină, link, observații)
NGFW Tip I — Cerințe tehnice minime obligatorii				
H1 — Cerințe Hardware				
H1.01	Echipamentul trebuie să fie 1U rack-mount 19" sau versiunea compactă, dotat cu kit de instalare în 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+ (10 Gbps).			
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 compatibil cu rețeaua de curent electric AC 220V, 50/60 Hz.			
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 (redundanță totală), cât și în mod Active-Active (distribuția sarcinii/load balancing), prin interconectarea cu un al doilea echipament identic. • Sincronizarea datelor: sincronizare 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): la defectarea unității principale sau pierderea conectivității pe un port monitorizat, comutarea traficului către unitatea secundară trebuie să fie automată, sub o secundă (sub-second), fără a întrerupe sesiunile active (stateful failover). • Monitorizarea legăturilor (Interface Monitoring): monitorizarea stării link-urilor critice (WAN/LAN); dacă un link pică pe unitatea activă, clusterul transferă automat rolul de „Master" către unitatea cu link-urile funcționale. • Management Unificat: administrarea clusterului HA printr-o singură adresă IP de management, indiferent de unitatea activă. • Actualizări fără întrerupere (Non-Disruptive Upgrade): actualizarea firmware-ului în cluster fără 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 Intruziuni, Antivirus și Control Aplicație activat.			
H1.10	Echipamentul trebuie să poată asigura criptare IPsec minim 20 Gbps.			
H1.11	Echipamentul trebuie să poată asigura minim 2M (milioane) de sesiuni TCP concurente.			
H1.12	Echipamentul trebuie să poată asigura minim 100.000 sesiuni noi/secundă.			
H1.13	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.			
H1.14	Echipamentul trebuie să poată asigura direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).			
H1.15	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.			
C1 — Cerințe funcționale				
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 Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS.			
C1.04	Echipamentul trebuie să suporte protocoale de tunelare, cel puțin: 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 locație.			
C1.06	Echipamentul trebuie să poată 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 și 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), cel puțin: RIPv2/ng, OSPFv2/v3, IS-IS și BGPv4 (iBGP/eBGP), atât pentru IPv4 cât și IPv6, rutarea bazată pe politici (PBR) și rutarea multicast (PIM-SM/DM).			
C1.10	Echipamentul trebuie să suporte Data Leak Prevention (DLP).			
C1.11	Echipamentul trebuie să suporte segmentarea virtuală în cel puțin 10 instanțe logice/virtuale independente (ex.: VDOM, Contexts, Virtual Systems sau echivalent), pentru izolarea completă a traficului între diferite departamente sau entități.			
C1.12	La expirarea licențelor de securitate, echipamentul trebuie să-și păstreze funcționalitatea de bază (Firewall, Routing, VPN, SD-WAN, interfață de management) fără limitarea numărului de utilizatori sau a lățimii de bandă.			
NGFW Tip II — Cerințe tehnice minime obligatorii				

H2 — Cerințe Hardware				
H2.01	Echipamentul trebuie să fie 1U rack-mount 19”, cu adâncimea maximă de 500 mm.			
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+ (10 Gbps).			
H2.04	Echipamentul trebuie să aibă cel puțin 8 porturi optice SFP (1 Gbps).			
H2.05	Echipamentul trebuie să fie dotat cu 2 surse de alimentare redundante.			
H2.06	Echipamentul trebuie să fie compatibil cu rețeaua de curent electric AC 220V, 50/60 Hz.			
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 (redundanță totală), cât și în mod Active-Active (distribuția sarcinii/load balancing), prin interconectarea cu un al doilea echipament identic. • Sincronizarea datelor: sincronizare 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): la defectarea unității principale sau pierderea conectivității pe un port monitorizat, comutarea traficului către unitatea secundară trebuie să fie automată, sub o secundă (sub-second), fără a întrerupe sesiunile active (stateful failover). • Porturi dedicate High Availability: 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): monitorizarea stării link-urilor critice (WAN/LAN); dacă un link pică pe unitatea activă, clusterul transferă automat rolul de „Master” către unitatea cu link-urile funcționale. • Management Unificat: administrarea clusterului HA printr-o singură adresă IP de management, indiferent de unitatea activă. • Actualizări fără întrerupere (Non-Disruptive Upgrade): actualizarea firmware-ului în cluster fără 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.			
H2.10	Echipamentul trebuie să poată asigura Threat Protection minim 2,5 Gbps cu modulul de Intruziuni, Antivirus și Control Aplicație activat.			
H2.11	Echipamentul trebuie să poată asigura protecție NGFW minim 3 Gbps.			
H2.12	Echipamentul trebuie să poată asigura criptare IPsec minim 25 Gbps.			
H2.13	Echipamentul trebuie să poată asigura minim 2M (milioane) de sesiuni TCP concurente.			
H2.14	Echipamentul trebuie să poată asigura minim 120.000 sesiuni noi/secundă.			
H2.15	Echipamentul trebuie să poată asigura inspecția SSL minim 3 Gbps.			
H2.16	Echipamentul trebuie să asigure capacitatea de a inspecta traficul criptat (HTTPS/SSL/TLS 1.3) fără degradarea critică a performanței.			
H2.17	Echipamentul trebuie să poată asigura direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).			
H2.18	Echipamentul trebuie să poată actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS.			
H2.19	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.			
C2 — Cerințe funcționale				
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 Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS.			
C2.04	Echipamentul trebuie să suporte protocoale de tunelare, cel puțin: 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 să poată 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 și 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), cel puțin: RIPv2/ng, OSPFv2/v3, IS-IS și BGPv4 (iBGP/eBGP), atât pentru IPv4 cât și IPv6, rutarea bazată pe politici (PBR) și rutarea multicast (PIM-SM/DM).			
C2.10	Echipamentul trebuie să suporte Data Leak Prevention (DLP).			
C2.11	Echipamentul trebuie să suporte segmentarea virtuală în cel puțin 10 instanțe logice independente (Virtual Domains / VDOMs sau echivalent), pentru izolarea completă a traficului între diferite departamente sau entități.			
C2.12	Funcționalul echipamentului nu trebuie să fie afectat la expirarea suportului de la producător, cu excepția actualizărilor de securitate.			
NGFW Tip III — Cerințe tehnice minime obligatorii				
H3 — Cerințe Hardware				
H3.01	Echipamentul trebuie să fie 1U rack-mount 19”, cu adâncimea maximă de 500 mm.			
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+ (10 Gbps).			
H3.04	Echipamentul trebuie să aibă cel puțin 8 porturi optice SFP (1 Gbps).			
H3.05	Echipamentul trebuie să fie dotat cu 2 surse de alimentare.			
H3.06	Echipamentul trebuie să fie compatibil cu rețeaua de curent electric 220V AC, 50/60 Hz.			

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 (redundanță totală), cât și în mod Active-Active (distribuția sarcinii/load balancing), prin interconectarea cu un al doilea echipament identic. • Sincronizarea datelor: sincronizare 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): la defectarea unității principale sau pierderea conectivității pe un port monitorizat, comutarea traficului către unitatea secundară trebuie să fie automată, sub o secundă (sub-second), fără a întrerupe sesiunile active (stateful failover). • Porturi dedicate High Availability: 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): monitorizarea stării link-urilor critice (WAN/LAN); dacă un link pică pe unitatea activă, clusterul transferă automat rolul de „Master” către unitatea cu link-urile funcționale. • Management Unificat: administrarea clusterului HA printr-o singură adresă IP de management, indiferent de unitatea activă. • Actualizări fără întrerupere (Non-Disruptive Upgrade): actualizarea firmware-ului în cluster fără 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.			
H3.10	Echipamentul trebuie să poată asigura Threat Protection minim 6 Gbps cu modulul de Intruziuni, Antivirus și Control Aplicație activat.			
H3.11	Echipamentul trebuie să poată asigura protecție NGFW minim 6 Gbps.			
H3.12	Echipamentul trebuie să poată asigura criptare IPsec minim 35 Gbps.			
H3.13	Echipamentul trebuie să poată asigura minim 5M (milioane) de sesiuni TCP concurente.			
H3.14	Echipamentul trebuie să poată asigura minim 200.000 sesiuni noi/secundă.			
H3.15	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.			
H3.16	Echipamentul trebuie să poată asigura direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).			
H3.17	Echipamentul trebuie să poată actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS.			
H3.18	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.			
C3 — Cerințe funcționale				
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 Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS.			
C3.04	Echipamentul trebuie să suporte protocoale de tunelare, cel puțin: 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 locație.			
C3.06	Echipamentul trebuie să poată 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 și 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), cel puțin: RIPv2/ng, OSPFv2/v3, IS-IS și BGPv4 (iBGP/eBGP), atât pentru IPv4 cât și IPv6, rutarea bazată pe politici (PBR) și rutarea multicast (PIM-SM/DM).			
C3.10	Echipamentul trebuie să suporte Data Leak Prevention (DLP).			
C3.11	Echipamentul trebuie să suporte segmentarea virtuală în cel puțin 10 instanțe logice independente (Virtual Domains / VDOMs sau echivalent), pentru izolarea completă a traficului între diferite departamente sau entități.			
C3.12	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).			