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

Tabela de conformitate — Achiziție echipamente NGFW (STAAP)

Anexă la Caietul de sarcini

1. Date de identificare a ofertantului

Denumirea ofertantului:	SC RAPID LINK SRL
IDNO / cod fiscal:	1007600035161
Persoana de contact / funcția:	Baciu Victor, Administrator
Producătorul echipamentelor ofertate:	Fortinet, Inc., SUA
Model ofertat — NGFW Tip I:	FortiGate-90G Hardware, FG-90G-BDL-950-12
Model ofertat — NGFW Tip II:	FortiGate-120G Hardware, FG-120G-BDL-950-12
Model ofertat — NGFW Tip III:	FortiGate-200G Hardware, FG-200G-BDL-950-12
Data:	16.07.2026

2. Lista bunurilor propuse achiziționării

Denumirea	Cantitate (buc.)
NGFW Tip I	50
NGFW Tip II	25
NGFW Tip III	28
TOTAL	**103**

3. Instrucțiuni de completare

• Cerințele din fila „Tabela de conformitate” sunt minime și obligatorii. Ofertantul completează fiecare poziție.

• Coloana „Conformitate” se completează din lista derulantă cu „Conform” sau „Neconform”. Celulele se colorează automat: verde = Conform, roșu = Neconform.
• În coloana „Produsul / modelul ofertat” se indică o singură dată, pentru fiecare tip (celulă unică pe tip), modelul/echipamentul ofertat — separat pentru NGFW Tip I, Tip II și Tip III.

• În coloana „Justificare / referință” se indică dovada conformității: denumirea documentului (datasheet/manual), numărul paginii/secțiunii și/sau link-ul oficial al producătorului.
• Mențiunea „Conform” fără referință verificabilă poate fi considerată neconcludentă la evaluare.

• O singură poziție „Neconform” sau necompletată la o cerință obligatorie poate atrage descalificarea ofertei.

• Tabelul de sumar de mai jos se actualizează automat pe baza completărilor din fila „Tabela de conformitate”.

4. Sumar conformitate (calculat automat)

Secțiune	Total cerințe	Conform	Neconform	% Conform
H1 — Hardware Tip I	15	15	0	100,0%
C1 — Funcționale Tip I	12	12	0	100,0%
H2 — Hardware Tip II	19	19	0	100,0%
C2 — Funcționale Tip II	12	12	0	100,0%
H3 — Hardware Tip III	18	18	0	100,0%
C3 — Funcționale Tip III	12	12	0	100,0%
TOTAL GENERAL	**88**	**88**	**0**	**100,0%**
OFERTĂ CONFORMĂ — toate cerințele sunt acoperite				

Numele, prenumele și funcția reprezentantului împuternicit:

Baciu Victor	**Semnătura / L.Ș.:**

Digitally signed by Baciu Victor
Date: 2026.07.16 08:19:58 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

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 1 — 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.	FortiGate-90G Hardware, FG-90G-BDL-950-12	Conform	Echipamentul este 1U rack-mount 19" dotat kit de instalare in rack. Mounting Ear brackets for FG-90/91G (conform "Optional Accessories" din datasheet-ul atasat)
H1.02	Echipamentul trebuie să aibă cel puțin 8 porturi RJ45 10/100/1000 Mbps.		Conform	Echipamentul are 8 porturi RJ45 10/100/1000 Mbps(conform datasheet-ului atasat)
H1.03	Echipamentul trebuie să aibă cel puțin 2 porturi optice SFP+ (10 Gbps).		Conform	Echipamentul are 2 porturi optice SFP+ (10Gbps)(conform datasheet-ului atasat)
H1.04	Echipamentul trebuie să aibă și consolă.		Conform	Echipamentul include consolă(conform datasheet-ului atasat)
H1.05	Echipamentul trebuie să fie dotat cu 2 surse de alimentare redundante.		Conform	Echipamentul este dotat cu 2 surse de alimentare redundante. Un adaptor de alimentare este inclus în complectul standard, iar al doilea adaptor de alimentare original a fost adăugat suplimentar. (conform "Optional Accessories" din datasheet-ul atasat)
H1.06	Echipamentul trebuie să fie compatibil cu rețeaua de curent electric AC 220V, 50/60 Hz.		Conform	Echipamentul este compatibile cu rețeaua de curent electric AC220V AC 50/60Hz.(conform datasheet-ului atasat)
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).		Conform	Echipamentul ofertat suporta configurarea în regim de Disponibilitate Sporită (High Availability - HA), respectând următoarele cerințe(conform datasheet-ului atasat): ●Moduri de operare: Permite 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 asigură 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 se va realiza automat, în mai puțin de 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 va transfera automat rolul de "Master" către unitatea care are link-urile funcționale. ● Management Unificat: Administrarea clusterului de tip HA se face 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).		Conform	Echipamentul asigură Firewall 20 Gbps (pentru pachete de 1518 bytes)(conform datasheet-ului atasat)
H1.09	Echipamentul trebuie să poată asigura Threat Protection minim 2 Gbps cu modulul de Intruziuni, Antivirus și Control Aplicație activat.		Conform	Echipamentul asigură Threat Protection 2 Gbps cu modulul de Intrusiuni , Antivirus și Control Aplicație activat(conform datasheet-ului atasat)
H1.10	Echipamentul trebuie să poată asigura criptare IPsec minim 20 Gbps.		Conform	Echipamentul asigură criptare IPsec 20 Gbps(conform datasheet-ului atasat)
H1.11	Echipamentul trebuie să poată asigura minim 2M (milioane) de sesiuni TCP concurente.		Conform	Echipamentul asigură minim 2M (milion) de sesiuni TCP concurente(conform datasheet-ului atasat)
H1.12	Echipamentul trebuie să poată asigura minim 100.000 sesiuni noi/secundă.		Conform	Echipamentul asigură minim 100000 sesiuni noi/secundă(conform datasheet-ului atasat)
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.		Conform	Echipamentul asigură un throughput pentru inspecția traficului criptat (SSL Inspection/Deep Packet Inspection) de 2 Gbps, cu suport obligatoriu pentru protocolul TLS 1.3.(conform datasheet-ului atasat)
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).		Conform	Echipamentul asigură direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).(conform datasheet-ului atasat)
H1.15	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.		Conform	Echipamentul dispune de suport de la producător de 1 an.
C1 — Cerințe funcționale				
C1.01	Echipamentele trebuie să susțină IEEE 802.1Q VLAN.	FortiGate-90G Hardware,	Conform	Echipamentele susțin IEEE 802.1Q VLAN.(conform datasheet-ului atasat)
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.		Conform	Agregare: Suport pentru IEEE 802.3ad (LACP) cu capacitatea de a grupa până la 4 porturi de 1G/10G într-un singur canal logic(conform datasheet-ului atasat)
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.		Conform	Echipamentele susțin Autentificare prin RADIUS, TACACS+, SSH v2, SNMP v3 și suport pentru Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS(conform datasheet-ului atasat)
C1.04	Echipamentul trebuie să suporte protocoale de tunelare, cel puțin: GRE, IPIP, L2TP, VxLAN.		Conform	Echipamentul suportă protocoalele de tunelare (conform datasheet-ului atasat)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 locație.		Conform	Echipamentul suportă 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(conform datasheet-ului atasat)
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.	FortiGate-90G Hardware,	Conform	Echipamentul au 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.(conform datasheet-ului atasat)

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).	FG-90G-BDL-950-12	Conform	Echipamentul include o interfață grafică (GUI) intuitivă care să permită vizualizarea în timp real a topologiei de rețea, a aplicațiilor utilizate (Application Control)(conform datasheet-ului atasat)
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.		Conform	Echipamentul suportă "Forward Error Correction" (FEC) şi "Packet Duplication" pentru a asigura calitatea aplicațiilor critice (VoIP, Video) pe legături WAN instabile(conform datasheet-ului atasat)
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).		Conform	Echipamentul suportă protocoale de rutare dinamică bazate pe standarde deschise (IETF), incluzând: RIPv2/ng, OSPFv2/v3, IS-IS şi BGPv4 (iBGP/eBGP), atât pentru IPv4 cât şi pentru IPv6, rutarea bazată pe politici (Policy-Based Routing - PBR) şi rutarea multicast (PIM-SM/DM)(conform datasheet-ului atasat)
C1.10	Echipamentul trebuie să suporte Data Leak Prevention (DLP).		Conform	Echipamentul suportă Data Leak Prevention (DLP)(conform datasheet-ului atasat)
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.		Conform	Echipamentul suporta segmentarea virtuală în 10 instanțe logice/virtuale independente (ex: VDOM, Contexts, Virtual Systems sau echivalent), pentru a permite izolarea completă a traficului între diferite departamente sau entități(conform datasheet-ului atasat)
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.		Conform	La expirarea licențelor de securitate, echipamentul va păstra funcționalitatea de bază (Firewall, Routing, VPN, SD-WAN, interfață de management) fără limitarea numărului de utilizatori sau a lățimii de bandă(conform datasheet-ului atasat)
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.	FortiGate-120G Hardware, FG-120G-BDL-950-12	Conform	Echipamentul este 1U rack-mount 19" cu adâncimea sub 500mm(conform datasheet-ului atasat)
H2.02	Echipamentul trebuie să aibă cel puțin 12 porturi RJ45 10/100/1000 Mbps.		Conform	Echipamentul are 12 porturi RJ45 10/100/1000 Mbps(conform datasheet-ului atasat)
H2.03	Echipamentul trebuie să aibă cel puțin 4 porturi optice SFP+ (10 Gbps).		Conform	Echipamentul are 4 porturi optice SFP+ (10Gbps)(conform datasheet-ului atasat)
H2.04	Echipamentul trebuie să aibă cel puțin 8 porturi optice SFP (1 Gbps).		Conform	Echipamentul are 8 porturi optice SFP (1Gbps)(conform datasheet-ului atasat)
H2.05	Echipamentul trebuie să fie dotat cu 2 surse de alimentare redundante.		Conform	Echipamentul este dotat cu 2 surse de alimentare redundante(conform datasheet-ului atasat)
H2.06	Echipamentul trebuie să fie compatibil cu rețeaua de curent electric AC 220V, 50/60 Hz.		Conform	Echipamentul este compatibil cu rețeaua de curent electric AC220V AC 50/60Hz.(conform datasheet-ului atasat)
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).		Conform	Echipamentul ofertat suportă configurarea în regim de Disponibilitate Sporită (High Availability - HA), respectând următoarele cerințe(conform datasheet-ului atasat): ●Moduri de operare: Permite 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 asigură 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 se realizează automat, în mai puțin de o secundă (sub-second failover), fără a întrerupe sesiunile active de utilizator (stateful failover). ●Porturi dedicate High Availability: Echipamentul dispune 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 transferă automat rolul de "Master" către unitatea care are link-urile funcționale. ●Management Unificat: Administrarea clusterului de tip HA se face 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.		Conform	Echipamentul asigură o latență ultra-scăzută de maxim 10 microsecunde în regim de firewall.(conform datasheet-ului atasat)
H2.09	Echipamentul trebuie să poată asigura Firewall minim 25 Gbps.		Conform	Echipamentul asigură Firewall 25 Gbps(conform datasheet-ului atasat)
H2.10	Echipamentul trebuie să poată asigura Threat Protection minim 2,5 Gbps cu modulul de Intruziuni, Antivirus și Control Aplicație activat.		Conform	Echipamentul asigură Threat Protection 2.5 Gbps cu modulul de Intrusiuni , Antivirus şi Control Aplicație activat(conform datasheet-ului atasat)
H2.11	Echipamentul trebuie să poată asigura protecție NGFW minim 3 Gbps.		Conform	Echipamentul oferă protecție NGFW 3 Gbps(conform datasheet-ului atasat)
H2.12	Echipamentul trebuie să poată asigura criptare IPsec minim 25 Gbps.		Conform	Echipamentul asigura criptare IPsec 25 Gbps(conform datasheet-ului atasat)
H2.13	Echipamentul trebuie să poată asigura minim 2M (milioane) de sesiuni TCP concurente.		Conform	Echipamentul asigura minim 2M (milioane) de sesiuni TCP concurente(conform datasheet-ului atasat)
H2.14	Echipamentul trebuie să poată asigura minim 120.000 sesiuni noi/secundă.		Conform	Echipamentul asigura minim 120000 sesiuni noi/secundă(conform datasheet-ului atasat)
H2.15	Echipamentul trebuie să poată asigura inspecția SSL minim 3 Gbps.		Conform	Echipamentul asigură inspecția SSL 3 Gbps(conform datasheet-ului atasat)
H2.16	Echipamentul trebuie să asigure capacitatea de a inspecta traficul criptat (HTTPS/SSL/TLS 1.3) fără degradarea critică a performanței.		Conform	Echipamentul asigură capacitatea de a inspecta traficul criptat (HTTPS/SSL/TLS 1.3) fără degradarea critică a performanțe(conform datasheet-ului atasat)
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).		Conform	Echipamentul asigură direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).(conform datasheet-ului atasat)
H2.18	Echipamentul trebuie să poată actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS.		Conform	Echipamentul poate actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS(conform datasheet-ului atasat)
H2.19	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.		Conform	Echipamentul dispune de suport de la producător de 1 an.
C2 — Cerințe funcționale				
C2.01	Echipamentele trebuie să susțină IEEE 802.1Q VLAN.		Conform	Echipamentele susține IEEE 802.1Q VLAN.(conform datasheet-ului atasat)
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.		Conform	Agregare: Suport pentru IEEE 802.3ad (LACP) cu capacitatea de a grupa până la 8 porturi de 1G/10G într-un singur canal logic(conform datasheet-ului atasat)
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.		Conform	Echipamentele susține Autentificare prin RADIUS, TACACS+, SSH v2, SNMP v3 şi suport pentru Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS(conform datasheet-ului atasat)

C2.04	Echipamentul trebuie să suporte protocoale de tunelare, cel puțin: GRE, IPIP, L2TP, VxLAN.	FortiGate-120G Hardware, FG-120G-BDL-950-12	Conform	Echipamentul suportă protocoalele de tunelare(conform datasheet-ului atasat) 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).		Conform	Funcționalitatea ZTNA (Zero Trust Network Access) este 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).(conform datasheet-ului atasat)
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.		Conform	Echipamentul oferă 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.(conform datasheet-ului atasat)
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).		Conform	Echipamentul include o interfață grafică (GUI) intuitivă care permite vizualizarea în timp real a topologiei de rețea, a aplicațiilor utilizate (Application Control)(conform datasheet-ului atasat)
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.		Conform	Echipamentul suportă "Forward Error Correction" (FEC) și "Packet Duplication" pentru a asigura calitatea aplicațiilor critice (VoIP, Video) pe legături WAN instabile(conform datasheet-ului atasat)
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).		Conform	Echipamentul suportă protocoale de rutare dinamică bazate pe standarde deschise (IETF), incluzând: 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)(conform datasheet-ului atasat)
C2.10	Echipamentul trebuie să suporte Data Leak Prevention (DLP).		Conform	Echipamentul suportă Data Leak Prevention (DLP)(conform datasheet-ului atasat)
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.		Conform	Echipamentul suportă segmentarea virtuală în 10 instanțe logice independente (Virtual Domains / VDOMs sau echivalent), pentru a permite izolarea completă a traficului între diferite departamente sau entități(conform datasheet-ului atasat)
C2.12	Funcționalul echipamentului nu trebuie să fie afectat la expirarea suportului de la producător, cu excepția actualizărilor de securitate.		Conform	Funcționalul echipamentului nu va fi afectat la expirarea suportului de la producător cu excepția actualizărilor de securitate(conform datasheet-ului atasat)
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.	FortiGate-200G Hardware, FG-200G-BDL-950-12	Conform	Echipamentul este 1U rack-mount 19” cu adâncimea sub 500mm(conform datasheet-ului atasat)
H3.02	Echipamentul trebuie să aibă cel puțin 12 porturi RJ45 10/100/1000 Mbps.		Conform	Echipamentul are 12 porturi RJ45 10/100/1000 Mbps(conform datasheet-ului atasat)
H3.03	Echipamentul trebuie să aibă cel puțin 4 porturi optice SFP+ (10 Gbps).		Conform	Echipamentul are 4 porturi optice SFP+ (10Gbps)(conform datasheet-ului atasat)
H3.04	Echipamentul trebuie să aibă cel puțin 8 porturi optice SFP (1 Gbps).		Conform	Echipamentul are 8 porturi optice SFP (1Gbps)(conform datasheet-ului atasat)
H3.05	Echipamentul trebuie să fie dotat cu 2 surse de alimentare.		Conform	Echipamentul este dotat cu 2 surse de alimentare(conform datasheet-ului atasat)
H3.06	Echipamentul trebuie să fie compatibil cu rețeaua de curent electric 220V AC, 50/60 Hz.		Conform	Echipamentul este compatibil cu rețeaua de curent electric 220V AC 50/60Hz(conform datasheet-ului atasat)
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).		Conform	Echipamentul ofertat suportă configurarea în regim de Disponibilitate Sporită (High Availability - HA), respectând următoarele cerințe(conform datasheet-ului atasat): ●Moduri de operare: permite 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 asigură 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 se realizează automat, sub o secundă (sub-second failover), fără a întrerupe sesiunile active de utilizator (stateful failover). ●Porturi dedicate High Availability: Echipamentul dispune 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 va transfera automat rolul de "Master" către unitatea care are link-urile funcționale. Management Unificat: Administrarea clusterului de tip HA se face 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.		Conform	Echipamentul asigură o latență ultra-scăzută de maxim 10 microsecunde în regim de firewall.(conform datasheet-ului atasat)
H3.09	Echipamentul trebuie să poată asigura Firewall minim 35 Gbps.		Conform	Echipamentul asigură Firewall 35 Gbps(conform datasheet-ului atasat)
H3.10	Echipamentul trebuie să poată asigura Threat Protection minim 6 Gbps cu modulul de Intruziuni, Antivirus și Control Aplicație activat.		Conform	Echipamentul poate asigura Threat Protection minim 6 Gbps cu modulul de Intrusiuni , Antivirus și Control Aplicație activat(conform datasheet-ului atasat)
H3.11	Echipamentul trebuie să poată asigura protecție NGFW minim 6 Gbps.		Conform	Echipamentul poate asigura protecție NGFW 6 Gbps(conform datasheet-ului atasat)
H3.12	Echipamentul trebuie să poată asigura criptare IPsec minim 35 Gbps.		Conform	Echipamentul poate asigura criptare IPsec 35 Gbps(conform datasheet-ului atasat)
H3.13	Echipamentul trebuie să poată asigura minim 5M (milioane) de sesiuni TCP concurente.		Conform	Echipamentul poate asigura minim 5M (milioane) de sesiuni TCP concurente(conform datasheet-ului atasat)
H3.14	Echipamentul trebuie să poată asigura minim 200.000 sesiuni noi/secundă.		Conform	Echipamentul poate asigura minim 200000 sesiuni noi/secundă(conform datasheet-ului atasat)
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.		Conform	Echipamentul asigură un throughput pentru inspecția traficului criptat (SSL Inspection/Deep Inspection) de 6 Gbps, cu suport obligatoriu pentru protocolul TLS 1.3.(conform datasheet-ului atasat)
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).		Conform	Echipamentul asigură direcționarea inteligentă a traficului pe multiple legături WAN în funcție de calitatea link-ului (jitter, latență, pierderi de pachete).(conform datasheet-ului atasat)
H3.17	Echipamentul trebuie să poată actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS.		Conform	Echipamentul poate actualiza baza de date cu semnături în timp real, cu protecție împotriva atacurilor de tip DoS/DDoS(conform datasheet-ului atasat)
H3.18	Echipamentul trebuie să dispună de suport de la producător de minim 1 an.		Conform	Echipamentul dispune de suport de la producător de 1 an.

C3 — Cerințe funcționale				
C3.01	Echipamentele trebuie să susțină IEEE 802.1Q VLAN.	FortiGate-200G Hardware, FG-200G-BDL-950-12	Conform	Echipamentele susține IEEE 802.1Q VLAN.(conform datasheet-ului atasat)
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.		Conform	Agregare: Suport pentru IEEE 802.3ad (LACP) cu capacitatea de a grupa până la 8 porturi de 1G/10G într-un singur canal logic(conform datasheet-ului atasat)
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.		Conform	Echipamentele susține Autentificare prin RADIUS, TACACS+, SSH v2, SNMP v3 și suport pentru Control Plane Policing (CoPP) pentru protecția procesorului împotriva atacurilor DoS(conform datasheet-ului atasat)
C3.04	Echipamentul trebuie să suporte protocoale de tunelare, cel puțin: GRE, IPIP, L2TP, VxLAN.		Conform	Echipamentul suportă protocoalele de tunelare cum ar fi(conform datasheet-ului atasat): ●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.		Conform	Echipamentul suportă 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(conform datasheet-ului atasat)
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.		Conform	Echipamentul oferă 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.(conform datasheet-ului atasat)
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).		Conform	Echipamentul include o interfață grafică (GUI) intuitivă care să permită vizualizarea în timp real a topologiei de rețea, a aplicațiilor utilizate (Application Control)(conform datasheet-ului atasat)
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.		Conform	Echipamentul suportă "Forward Error Correction" (FEC) şi "Packet Duplication" pentru a asigura calitatea aplicațiilor critice (VoIP, Video) pe legături WAN instabile(conform datasheet-ului atasat)
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).		Conform	Echipamentul suportă protocoale de rutare dinamică bazate pe standarde deschise (IETF), incluzând: 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)(conform datasheet-ului atasat)
C3.10	Echipamentul trebuie să suporte Data Leak Prevention (DLP).		Conform	Echipamentul suportă Data Leak Prevention (DLP)(conform datasheet-ului atasat)
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.		Conform	Echipamentul suportă segmentarea virtuală în 10 instanțe logice independente (Virtual Domains / VDOMs sau echivalent), pentru a permite izolarea completă a traficului între diferite departamente sau entități(conform datasheet-ului atasat)
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).		Conform	Funcționalitatea de bază a echipamentului (rutare, firewall, VPN) nu este condiționată sau blocată la expirarea abonamentelor de suport/securitate (cu excepția actualizărilor de semnături)(conform datasheet-ului atasat)