ANEXA NR. 1 - CERINȚE TEHNICE *ECHIPAMENT DE PROCESARE*

Se va livra un echipament de procesare cu următoarele caracteristici:

CARACTERISTICĂ	CERINȚĂ TEHNICĂ MINIMALĂ
Procesor:	Tip: Intel Xeon Gold 6526Y sau configurație echivalentă din punct de vedere al performanței Frecvența minimă bază 2.5 GHz, Cache: 37 MB Număr de nuclee per procesor: 16 nuclee Număr de procesoare instalate: 2
Memorie:	Memorie instalată: 256 GB DDR4 ECC
Placa video	NVIDIA L4, PCIe, 72W, 24GB Passive, Single Wide Full Height GPU sau echivalent
Capacitate stocare:	Capacitate instalată: Minim 2 x 960 GB SSD SATA
Format	Rack-abil 19 inch
Identificare erori:	Afișaj LCD sau LED pentru semnalizarea erorilor globale
Sloturi:	2 sloturi PCI-Express x4 1 slot PCI-Express x16
Porturi integrate:	2 porturi USB 2.0 1 port serial 1 port VGA 2 porturi RJ45
Sursă de alimentare:	Minim 2 surse cu capacitate conform fisei tehnice producator Redundanță: Da, capabilitate hotplug Tensiune: suport pentru 220VAC / 50Hz
Ventilatoare:	2 ventilatoare hotplug, configurație redundantă
Interfețe Ethernet:	2 interfețe Ethernet 10 Gbit/s

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIE
NUMĂR 271 / DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 17.11.2025

Sistem de operare instalat:	Microsoft Windows Server
vSPhere Standard	Se vor licenția toate core-urile procesorului
Accesorii	kit de montare în rack
GARANȚIE	Perioada de garanție oferită confom caietului de sarcini. Oferită de către producătorul echipamentelor.
	HDD/SSD-urile care vor prezenta defecțiuni hardware pe perioada de derulare a garanției vor fi înlocuite cu alte HDD/SSD-uri (cu performante identice sau superioare) fără a fi returnate Furnizorului (indiferent de natura defectului).
	Atât HDD/SSD-urile care le înlocuiesc pe cele defecte, cât și cele defecte, rămân în proprietatea Beneficiarului.
NOTA	Echipamentele livrate vor fi noi. Nu se acceptă echipamentele remanufacturate și/sau care au în componență elemente care au fost folosite anterior.
	Documentele tehnice prezentate pentru susținerea ofertei vor fi acceptate exclusiv în limba română sau engleză.

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 17.11.2025

ANEXA NR. 2 - CERINȚE TEHNICE *ECHIPAMENT DE STOCARE*

Echipamentul de stocare trebuie să realizeze **extensia** capacității echipamentului de stocare conform următoarelor cerințe:

CARACTERISTICĂ TEHNICĂ	CERINȚA TEHNICĂ MINIMALĂ
Sertare de disk	Minim 2 Sertar de disk
Disk-uri montate	Minim 2x24 SSD SAS – 1.92 TB 2.5 12G
Extinderea capacității echipamentului de stocare Fujitsu Etenrus DX600 S5	Se va realiza exitenderea capacității echipamentului de stocare existent **Fujitsu Eternus DX600 S5** cu păstrarea capacității disk-urilor existente
Detalii instalare	Realizarea extinderii capacității echipamentului precum și a subansamblelor ofertate intră în sarcina exclusivă a furnizorului. Furnizorul va asigura realizarea extinderii capacității cu personal certificat/autorizat de producător.
Servicii incluse	Extinderea capacității va fi instalată și configurată de către furnizor fără oprirea echipamentului de stocare la care se atașează sertarele de disk-uri împreună cu toate disk-urile solicitate. Furnizorul, prin presonal calificat, va efectua toate testele necesare pentru asigurarea funcționării optime și continue a sistemului de stocare după realizarea acestor operațiuni. Furnziorul trebuie să se asigure că licențele instalate pe sistemul de stocare existent se vor păstra și după operațiunea de extindere a capacității , precum și că acestea vor asigura funcționalitățile cerute privind asiguraerea serviciilor de înaltă disponibilitate.
Alte accesorii	Vor fi asigurate de către furnizor toate accesoriile și licențele necesare instalării și configurării extensiei capacității sistemului de stocare existent **Fujitsu Eternus DX600 S5**, acestea intrând în sarcina exclusivă a acestuia.
Garanție	Minim 36 de luni
	SSD-urile care vor prezenta defecțiuni hardware pe perioada de derulare a garanției vor fi înlocuite cu alte SSD-uri (cu performanțe identice sau superioare) fără a fi returnate Furnizorului (indiferent de natura defectului).
Nota	Echipamentele livrate vor fi noi. Nu se acceptă echipamente remanufacturate și/sau care au în componență elemente care au fost folosite anterior.

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIE
NUMĂR 271 DATA 11.11.2025

ANEXA NR. 3 - CERINȚE TEHNICE *SWITCH ACCES TIP 1*

Switch Acces Tip 1 - se va livra 5 bucăți și vor avea următoarele specificații tehnice:

Cerințe tehnice generale	• Șasiu fix • Echipamentul trebuie sa conțină tag RFID, astfel încât utilizând un cititor RFID sa faciliteze gestionarea inventarului • Echipamentul sa suporte alimentare redundanta
Cerințe hardware obligatorii	• Memorie DRAM – minim 2 GB; • Memorie Flash – minim 4 GB; • Echipamentul trebuie sa aibă un mecanism prin care sa se valideze asocierea dintre hardware si software (in cazul in care hardware-ul sau software-ul nu este cel original sau a fost alterat, echipamentul sa identifice acest lucru)
Interfețe	• 48 de porturi de 10/100/1000 Mbps RJ45 • 4 porturi 1 Gbps SFP • Port Consola RJ45 • Port Consola USB • Echipamentul sa suporte conectarea unui modul dedicate de stack, cu suport pentru conectarea a 8 echipamente in stiva cu o lățime de banda agregatoare de 80Gbps per modul.
Performante	• Lărgimea de banda switching – 104 Gbps • Forwarding Rate – 77.38 Mpps • Adrese MAC – 16.000 • VLAN IDs – 4000 • Jumbo Frames – 9198 bytes
Cerințe privind sistemul de operare	• Sistemul de operare al echipamentului trebuie sa ofere support pentru configurare folosind API-uri deschise, NETCONF, RESTCONT, YANG • Suport pentru netflow/jflow/sflow neeșantionat (unsampled)
Power over Ethernet	• NU
Management	Autentificare TACACS+/RADIUS prin platforma Cisco ISE 3.X existenta in cadrul rețelei beneficiarului. • Suport pentru integrarea in platforma Cisco ISE pentru a putea primi automat de la aceasta reguli de autentificare si autorizare utilizatori si drepturi de acces in rețea pentru fiecare utilizator • Management prin platforma Cisco Catalyst Center existenta in cadrul rețelei beneficiarului.

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIE
NUMĂR 272 / DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

	• Prin integrarea in Platforma Cisco Catalyst Center se va realiza managementul fișierelor de configurare si a sistemelor de operare ale echipamentului ofertat
Protocoale suportate	• IEEE 802.1s • IEEE 802.1w • IEEE 802.1x inclusive CoA • IEEE 802.1x-Rev • IEEE 802.3ad • IEEE 802.3af • IEEE 802.3at • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10 Base-T Specification • IEEE 802.3u 100BASE-T specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • RMON I and II standards • SNPMv1, v2c and v3
Parametri alimentare	• Frecventa de funcționare: 50-60 Hz • Tensiunea de funcționare: 100-240 VAC
Mediu de funcționare	• Temperatura de funcționare: de la 0^0 la 40^0 C • Umiditate: de la 10 la 85%
Dimensiuni	• 19" montabil in rack (se va include si kit-ul de montare in rack) • Maxim 1 x RU înălțime
Cerințe generale	• Echipamentele, solutiile si licentele furnizate vor fi noi, neutilizate si nu sunt anunțate de producător ca fiind Enf of Sale/End-of-Life/End-of-Support. Nu se accepta echipamente folosite anterior, resigilate, remanufacturate • Echipamentele livrate vor fi însoțite de declarații de conformitate CE si certificate de garanție
Licențiere	• Echipamentul va conține următoarele funcționalități minime ce vor fi si licențiate: Layer 2, Routed Access (RIP, OSPF – 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, QoS, FHS, 802.1X, MACsec-128 • Sa permită următoarele protocoale (eventual prin licențiere ulterioara): IS-IS, VRF, VXLAN • Se vor livra si licențele necesare pentru autentificare si autorizarea utilizatorilor in Cisco ISE, minimum 48 de licențe per switch.

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

	• Echipamentul ofertat va folosi licențele existente in cadrul platformei existente Cisco Catalyst Center de la nivelul Beneficiarului.
Garanție si suport tehnic	• Garanția hardware si software a tuturor echipamentelor si modulelor din compunerea sistemului ofertat si livrat va fi de minim 36 de luni • In perioada de garanție a echipamentelor si soluțiilor, Furnizorul are obligația de a asigura, fără cheltuieli suplimentare din partea Beneficiarului, servicii de suport tehnic ce presupune inclusiv înlocuirea echipamentelor defecte, remedieri de natura software • Reparația este considerate finalizata in urma verificării ca funcționare defectuoasa a produsului a fost corectata. Furnizorul are obligația de a efectua toate operațiunile necesare punerii in funcțiune a echipamentului (instalare, configurare, integrare in infrastructura IT a beneficiarului), fără costuri suplimentare din partea Beneficiarului. • Toate piesele de schimb furnizate in perioada de garanție vor prelua perioada de garanție rămasa a echipamentului/modulului înlocuit si vor beneficia de aceleași condiții de reparații si suport tehnic ca si echipamentul achiziționat inițial • Suport pentru update-uri și patch-uri 36 luni • Se vor include toate serviciile necesare pentru asigurarea accesului direct al personalului Beneficiarului la site-ul producătorului pentru download de software si update-uri pe perioada garanției/suportului tehnic • Se va oferi posibilitatea accesului direct al personalului beneficiarului la site-ul producătorului in vederea deschiderii unor cazuri pentru depanarea problemelor apărute pe partea de software/hardware. Se va furniza ulterior, de către Beneficiar, contul de acces necesar în vederea asigurării serviciilor prezentate mai sus;

ANEXA NR. 4 - CERINȚE TEHNICE *SWITCH ACCES TIP 2*

Switch Acces Tip 2 - se va livra 5 bucăți și vor avea următoarele specificații tehnice:

Cerințe tehnice generale	• Șasiu fix • Echipamentul trebuie sa conțină tag RFID, astfel încât utilizând un cititor RFID sa faciliteze gestionarea inventarului
Cerințe hardware obligatorii	• Memorie DRAM – minim 4 GB; • Memorie Flash – minim 8 GB; • Echipamentul trebuie sa aiba un mecanism prin care sa se valideze asocierea dintre hardware si software (in cazul in care hardware-ul sau software-ul nu este cel original sau a fost alterat, echipamentul sa identifice acest lucru)
Interfețe	• 8 de porturi de 10/100/1000 Mbps RJ45 PoE+ • 2 porturi 1 Gbps SFP • 2 porturi 10 Gbps SFP+ • Port Consola RJ45 • Port Consola USB
Performante	• Lărgimea de banda switching – 60 Gbps • Forwarding Rate – 44.64 Mpps • Adrese MAC – 32.000 • VLAN IDs – 4000 • Jumbo Frames – 9198 bytes
Cerințe privind sistemul de operare	• Sistemul de operare al echipamentului trebuie sa ofere suport pentru configurare folosind API-uri deschise, NETCONF, RESTCONT, YANG • Suport pentru netflow/jflow/sflow neesantionat (unsampled)
Power over Ethernet	• DA, PoE+ 240W
Management	• Autentificare TACACS+/RADIUS prin platforma Cisco ISE 3.X existenta in cadrul rețelei beneficiarului. • Suport pentru integrarea in platforma Cisco ISE pentru a putea primi automat de la aceasta reguli de autentificare si autorizare utilizatori si drepturi de acces in rețea pentru fiecare utilizator • Management prin platforma Cisco Catalyst Center existenta in cadrul rețelei beneficiarului. • Prin integrarea in Platforma Cisco Catalyst Center se va realiza managementul fișierelor de configurare si a sistemelor de operare ale echipamentului ofertat
Protocoale suportate	• IEEE 802.1s

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

	• IEEE 802.1w • IEEE 802.1x inclusive CoA • IEEE 802.1x-Rev • IEEE 802.3ad • IEEE 802.3af • IEEE 802.3at • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10 Base-T Specification • IEEE 802.3u 100BASE-T specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • IEEE 802.3an 10GBase-T • RMON I and II standards • SNPMv1, v2c and v3
Parametri alimentare	• Frecventa de funcționare: 50-60 Hz • Tensiunea de funcționare: 100-240 VAC
Mediu de funcționare	• Temperatura de funcționare: de la 0^0 la 40^0 C • Umiditate: de la 10 la 85%
Dimensiuni	• 19" montabil in rack (se va include si kit-ul de montare in rack) • Maxim 1 x RU înălțime
Cerințe generale	• Echipamentele, soluțiile si licențele furnizate vor fi noi, neutilizate si nu sunt anunțate de producător ca fiind Enf of Sale/End-of-Life/End-of-Support. Nu se accepta echipamente folosite anterior, resigilate, remanufacturate • Echipamentele livrate vor fi însoțite de declarații de conformitate CE si certificate de garanție
Licențiere	• Echipamentul va conține următoarele funcționalități minime ce vor fi si licențiate: Layer 2, Routed Access (RIP, OSPF – 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, QoS, FHS, 802.1X, MACsec-128 • Sa permită următoarele protocoale (eventual prin licențiere ulterioara): IS-IS, VRF, VXLAN • Echipamentul ofertat va folosi licențele existente in cadrul platformei existente Cisco Catalyst Center de la nivelul Beneficiarului.
Garanție si suport tehnic	• Garanția hardware si software a tuturor echipamentelor si modulelor din compunerea sistemului ofertat si livrat va fi de minim 36 de luni

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

	• In perioada de garanție a echipamentelor si soluțiilor, Furnizorul are obligația de a asigura, fără cheltuieli suplimentare din partea Beneficiarului, servicii de suport tehnic ce presupune inclusiv înlocuirea echipamentelor defecte, remedieri de natura software • Reparația este considerate finalizata in urma verificării ca funcționare defectuoasa a produsului a fost corectata. Furnizorul are obligația de a efectua toate operațiunile necesare punerii in funcțiune a echipamentului (instalare, configurare, integrare in infrastructura IT a beneficiarului), fără costuri suplimentare din partea Beneficiarului. • Toate piesele de schimb furnizate in perioada de garanție vor prelua perioada de garanție rămasa a echipamentului/modulului înlocuit si vor beneficia de aceleași condiții de reparații si support tehnic ca si echipamentul achiziționat inițial • Suport pentru update-uri și patch-uri 36 luni • Se vor include toate serviciile necesare pentru asigurarea accesului direct al personalului Beneficiarului la site-ul producătorului pentru download de software si update-uri pe perioada garanției/suportului tehnic • Se va oferi posibilitatea accesului direct al personalului beneficiarului la site-ul producătorului in vederea deschiderii unor cazuri pentru depanarea problemelor apărute pe partea de software/hardware. Se va furniza ulterior, de către Beneficiar, contul de acces necesar în vederea asigurării serviciilor prezentate mai sus;

ANEXA NR. 5 - CERINȚE TEHNICE *SWITCH ACCES TIP 3*

Switch Acces Tip 3 - se va livra 1 bucată și va avea următoarele specificații tehnice:

Cerințe tehnice generale	• Șasiu modular • Echipamentul trebuie sa conțină tag RFID, astfel încât utilizând un cititor RFID sa faciliteze gestionarea inventarului • Echipamentul sa suporte alimentare redundanta (va fi livrat cu doua surse de alimentare si cablu de alimentare)
Cerințe hardware obligatorii	• Memorie DRAM – minim 8 GB; • Memorie Flash – minim 16 GB; • Echipamentul trebuie sa aibă un mecanism prin care sa se valideze asocierea dintre hardware si software (in cazul in care hardware-ul sau software-ul nu este cel original sau a fost alterat, echipamentul sa identifice acest lucru)
Interfețe	• 24 de porturi multigigabit UPOE (10G/5G/2.5G/1G/100M)RJ45 • Modul 8 porturi 10 Gbps SFP+ inclus • Port Consola RJ45 • Port Consola USB • Echipamentul să suporte conectarea unui modul dedicate de stack, cu suport pentru conectarea a 8 echipamente in stiva cu o lățime de banda agregatoare de 480Gbps per modul.
Performante	• Lărgimea de banda switching – 640 Gbps • Forwarding Rate – 476.19 Mpps • Adrese MAC – 32.000 • VLAN IDs – 4000 • Jumbo Frames – 9198 bytes • IPv6 routing entries – 16.000 • Multicat routing scale – 8.000 • ACL scale entries – 5.120 • Total number of IPv4 routes – 32.000
Cerințe privind sistemul de operare	• Sistemul de operare al echipamentului trebuie sa ofere suport pentru configurare folosind API-uri deschise, NETCONF, RESTCONT, YANG • Suport pentru netflow/jflow/sflow neeșantionat (unsampled)
UPOE	• DA, Cisco UPOE (60W per port) and IEEE 802.3bt Type 3 on all ports (24-port switch)

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

Management	• Autentificare TACACS+/RADIUS prin platforma Cisco ISE 3.X existenta in cadrul rețelei beneficiarului. • Suport pentru integrarea in platforma Cisco ISE pentru a putea primi automat de la aceasta reguli de autentificare și autorizare utilizatori și drepturi de acces în rețea pentru fiecare utilizator • Management prin platforma Cisco Catalyst Center existenta în cadrul rețelei beneficiarului. • Prin integrarea în Platforma Cisco Catalyst Center se va realiza managementul fișierelor de configurare și a sistemelor de operare ale echipamentului ofertat
Protocoale suportate	• IEEE 802.1s • IEEE 802.1w • IEEE 802.1x inclusive CoA • IEEE 802.1x-Rev • IEEE 802.3ad • IEEE 802.3af • IEEE 802.3at • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10 Base-T Specification • IEEE 802.3u 100BASE-T specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • IEEE 802.3bt • IEEE 802.3bz Multirate 2.5G/5G • IEEE 802.3an 10G BASE-T • RMON I and II standards • SNPMv1, v2c and v3
Parametri alimentare	• Frecventa de funcționare: 50-60 Hz • Tensiunea de funcționare: 100-240 VAC
Mediu de funcționare	• Temperatura de funcționare: de la 0^0 la 40^0 C • Umiditate: de la 10 la 85%
Dimensiuni	• 19" montabil in rack (se va include si kit-ul de montare in rack) • Maxim 1 x RU înălțime
Module SFP	• 2 module 10 GBase SFP+ optic, SFP-10G-SR-X, conector compatibil LC, fabricate de producătorul echipamentului ofertat
Cerințe generale	• Echipamentele, soluțiile si licențele furnizate vor fi noi, neutilizate si nu sunt anunțate de producător ca fiind Enf of Sale/End-of-Life/End-of-Support. Nu se accepta

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

	echipamente folosite anterior, resigilate, remanufacturate • Echipamentele livrate vor fi însoțite de declarații de conformitate CE si certificate de garanție
Licențiere	• Echipamentul va conține următoarele funcționalități minime ce vor fi si licențiate: Layer 2, Routed Access (RIP, OSPF – 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, QoS, FHS, 802.1X, MACsec-128 • Sa permită următoarele protocoale (eventual prin licențiere ulterioara): IS-IS, VRF, VXLAN • Se vor livra si licențele necesare pentru autentificare si autorizarea utilizatorilor in Cisco ISE, minimum 24 de licențe per switch. • Echipamentul ofertat va folosi licențele existente in cadrul platformei existente Cisco Catalyst Center de la nivelul Beneficiarului.
Garanție si suport tehnic	• Garanția hardware si software a tuturor echipamentelor si modulelor din compunerea sistemului ofertat si livrat va fi de minim 36 de luni • In perioada de garanție a echipamentelor si soluțiilor, Furnizorul are obligația de a asigura, fără cheltuieli suplimentare din partea Beneficiarului, servicii de suport tehnic ce presupune inclusiv înlocuirea echipamentelor defecte, remedieri de natura software • Reparația este considerate finalizata in urma verificării ca funcționare defectuoasa a produsului a fost corectata. Furnizorul are obligația de a efectua toate operațiunile necesare punerii in funcțiune a echipamentului (instalare, configurare, integrare in infrastructura IT a beneficiarului), fără costuri suplimentare din partea Beneficiarului. • Toate piesele de schimb furnizate in perioada de garanție vor prelua perioada de garanție rămasa a echipamentului/modulului înlocuit si vor beneficia de aceleași condiții de reparații si suport tehnic ca si echipamentul achiziționat inițial • Suport pentru update-uri și patch-uri 36 luni • Se vor include toate serviciile necesare pentru asigurarea accesului direct al personalului Beneficiarului la site-ul producătorului pentru download de software si update-uri pe perioada garanției/suportului tehnic • Se va oferi posibilitatea accesului direct al personalului beneficiarului la site-ul producătorului in vederea

	deschiderii unor cazuri pentru depanarea problemelor apărute pe partea de software/hardware. Se va furniza ulterior, de către Beneficiar, contul de acces necesar în vederea asigurării serviciilor prezentate mai sus;

ANEXA NR. 6 - CERINȚE TEHNICE *SOLUȚIE DE MANAGEMENT AL ACCESULUI LA REȚEA (NETWORK ACCESS MANAGEMENT SOLUTION)*

Soluție de management al accesului la rețea (Network Access Management Solution) - se va livra 1 bucată și va avea următoarele specificații tehnice:

1. Cerințe generale ale soluției	
1.1	Aplicație pentru managementul centralizat al identității si acces autorizat in rețele informatice a stațiilor de lucru, terminalelor mobile si alte echipamente conectate.
1.2	Funcții de AAA (autentificare, autorizare si accounting) prin protocol de tip RADIUS si TACACS+.
1.3	Funcționare cu echipamente sau aplicații virtualizate dedicate on premises.
1.4	Integrare cu soluții de web proxy si filtrare de conținut web .
1.5	Integrare cu echipamente de rețea wireless, cablate, de switching si de rutare.
1.6	Suport integral IPv6 pentru protocoalele de tip RADIUS si TACACS+.
1.7	Integrare cu echipamente de securitate de perimetru Firewall.
2. Certificări și garanții de autenticitate hardware si software	
2.1	Conform criteriilor FIPS 140-2.
2.2	Certificare Comon Criteria (EAL4) activa sau in proces de evaluare.
3. Suport pentru rularea aplicației pe sisteme de operare virtualizate utilizate de benficiar de tip:	
3.1	Vmware ESXi 6.5, 6.7, 7.x si Vmware cloud.
3.2	KVM on RedHat 7.x
3.3	Microsoft Hyper-V pe server 2012R2 sau versiuni superioare
3.4	Nutanix AHV
3.5	AWS
4. Funcții de scalabilitate, management si operare	
4.1	Accesul către aplicație din browser peste protocol securizat HTTPS fără limitări ale aplicațiilor ce pot accesa aplicația.
4.2	Adăugarea, gestionarea si monitorizarea tuturor utilizatorilor si dispozitivelor conectate, de la o singura consola si printr-o singura interfața de acces.
4.3	Funcționare ca server Radius pentru întreaga infrastructura de rețea, inclusiv pentru echipamentele ce nu implica accesul direct al utilizatorilor.
4.4	Aplicația de management va capta evenimente SNMP de la echipamentele configurate.
4.5	Aplicația va permite accesul utilizatorilor indiferent de tipul de echipament fix sau mobil prin care aceștia doresc acces, cum ar fi PC, laptop, smartphone, tablete.
4.6	Aplicația va asigura flexibilitatea in configurare prin care un echipament ce se conectează prin VPN sa aibă aplicate automat reguli mai stricte de acces, fata de regulile aplicate aceluiași echipament ce se conectează in sediu, prin cablu sau prin wireless.
4.7	Aplicația va asigura flexibilitatea operatorului sa configureze acces restricționat aceluiași echipament ce se conectează într-o locație distanta si nu in sediul principal, indiferent de tipul de conectivitate prin fir sau wireless.
4.8	Aplicația va permite urmărirea in mod curent si in istoric a fiecărui utilizator si device si a activității acestuia din punct de vedere autentificare si autorizare.

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIE
NUMĂR 272 / DATA 11.11.2025

4.9	Aplicația va permite funcționarea ca server de tip TACACS+, pentru autentificarea si autorizarea accesului utilizatorilor si administrării echipamentelor de rețea prin protocoale de administrare la distanta, in mod audiabil din aceeași consola de management.
4.10	Aplicația va permite autentificarea cu certificate digitale, autentificarea prin smart-card-uri de tip RSA SecurID, surse externe de autentificare precum ActiveDirectory, LDAP.
4.11	Aplicația va permite adăugarea mai multor servere ce conțin informații despre utilizatori, spre exemplu Active Directory, OpenRadius, pe care le va putea interoga secvențial pentru autentificarea cu succes a unui utilizator sau dispozitiv. De asemeni aplicația va trebui sa suporte integrarea cu mai multe servere Active Directory simultan, indiferent daca acestea au legătura de trust sau nu.
4.12	Aplicația va verifica in cazul certificatelor digitale, autenticitatea si validitatea la autoritatea emitenta prin protocol de tip OCSP.
4.13	Aplicația va expune informații de autentificare, tipul de dispozitiv, locația unde s-a autentificat dispozitivul, starea dispozitivului spre exemplu: autorizat sau in carantina, prin protocolul standard de partajare de date de tip XMPP Grid, descris in RFC8600 sau echivalent.
4.14	Aplicația va permite crearea, gestionarea si publicarea unei politici de securitate, unitara, administrata dintr-un singur loc iar apoi distribuita către infrastructura de rețea prin protocol de tip XMPP Grid. Administrarea si actualizarea politicii de securitate prin aplicație va trebui sa aibă efecte asupra infrastructurii de retea, aceasta din urma sa respecte politica de securitate publicata. Aplicația va permite urmărirea echipamentelor din infrastructura ce primesc politica de securitate publicata si aplicarea in timp real a acesteia. Infrastructura de rețea a se înțelege echipamente de switching, routing si Firewall.
4.15	Aplicația va putea scala prin arhitectura sa, centralizata sau distribuita, de la zeci de dispozitive, la sute de mii de dispozitive, fără ca instalarea inițială sa se schimbe ci doar sa se crească resursele mașinilor virtuale, sau sa se adauge instanțe noi ale aplicației cu roluri dedicate sau appliance-uri hardware cu aplicația preinstalata.
4.16	Aplicația va permite modificarea autorizării pentru un dispozitiv, direct către echipamentele de comunicații la care acel dispozitiv s-a conectat (funcția de change of authorization, CoA);
4.17	Funcție de autentificare temporara pentru utilizatori nestatornici, vizitatori, care au roluri definite de acces la aplicație dar au perioada clar determinata ca utilizatori. Utilizatorii pot primi nume de utilizator si parola cu drepturi de acces asociate, dar dupa expirarea perioadei de timp, numele de utilizator va fi șters automat.
4.18	Aplicația va permite absorbirea prin API sau prin protocol bine documentat, informații adiționale despre dispozitivele autentificate, de la alte platforme din rețea.
4.19	Aplicația va permite definirea de secvențe de autentificare si autorizare prin care dispozitivul conectat poate fi autentificat după cum urmează: 802.1x, MAB, WebAuth.sau echivalent
5. Funcții avansate de autorizare si partajare de informații (disponibile eventual prin licențiere ulterioară)	
5.1	Aplicația va realiza un audit al dispozitivelor ce incearca sa se conecteze si sa verifice daca acestea îndeplinesc criteriile prestabilite de securitate si stabilitate necesare functionarii in cadrul rețelei IT, înainte ca acestea sa aibă acces in rețea; In cazul in care

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / DATA 11.11.2025

	dispozitivele nu îndeplinesc criteriile prestabilite de securitate, aplicația va lua masuri de carantina si de izolare pana când dispozitivele trec prin procedura de remediere.
5.2	Aplicația va asigura recunoașterea fiecărui echipament in parte, îl va cataloga, va aplica un profil de echipament si in cooperare cu infrastructura de rețea, ii va oferi acces conform regulilor specifice acelui echipament.
5.3	In cazul in care detectează ca un dispozitiv este conectat dar nu a trecut de auditul intern de securitate, aplicația va pune la dispoziție pașii de remediere automat. Accesul dispozitivului in rețea va fi permis abia după remediere.
5.4	Aplicația va putea interacționa prin integrări cu alte soluții de securitate pentru automatizarea reacției in caz de incident si de comanda a carantinei pentru echipamentele suspicioase si predispuse compromiterii.
5.5	Aplicația va permite crearea, gestionarea si publicarea unei politici de securitate, unitara, administrata dintr-un singur loc iar apoi distribuita către infrastructura de rețea prin protocol XMPP Grid. Administrarea si actualizarea politicii de securitate prin aplicație va trebui sa aibă efecte asupra infrastructurii de rețea, aceasta din urma sa respecte politica de securitate publicata. Aplicația va permite urmărirea echipamentelor din infrastructura ce primesc politica de securitate publicata si aplicarea in timp real a acesteia. Infrastructura de rețea a se înțelege echipamente de switching, routing si Firewall.
6. Cerințe de administrare, logare si control de la distanta	
6.1	Aplicația va permite administratorilor acces la consola prin SSH.
6.2	Aplicația va permite definirea de roluri bine determinate care operatori, cu delimitări asupra stațiilor de lucru, politicii de inspecție sau a politicii de alertare. Un operator cu drepturi doar pe un subset de stații de lucru, va avea acces doar la politicile specifice acelui subset, cat si la setul de date, evenimente si rapoarte care este de asemeni specific acelui subset de stații de lucru.
6.3	Aplicația va expune prin API REST bine documentat, informațiile de autentificare, IP, hostname, tipul de dispozitiv, locația unde s-a autentificat dispozitivul, alte informații asociate procesului de autentificare. Aceste informații trebuie sa fie integrabile într-o aplicație de tip SIEM.
7. Licențiere si perioada de garanție	
7.1	Telemetria de securitate si licențele necesare pentru o perioada de 3 ani (licențele vor fi perpetue sau vor fi subscripții valabile pe toata perioada de garanție ofertata)
7.2	Numărul de dispozitive protejate: 1000
7.3	Numărul de instanțe ale aplicației: 1
7.4	Suport software pe o perioada de 3 (trei) ani, acoperind dreptul de a face update–uri software la aplicațiile ce compun soluția ofertata ori de câte ori este necesar precum si acces direct la site-ul producătorului pentru a deschide direct, ori de cate ori este necesar cazuri de suport cu acesta; Se vor preciza part-number-ul (–ele) care asigura condițiile de garanție hardware si suport software mai sus menționate.
8. Servicii implementare (ce vor trebui prestate de Ofertant)	
8.1	**Planificare si pregătire** • Evaluarea infrastructurii existente: Ofertantul va evalua dispozitivele de rețea si infrastructura existenta pentru a determina compatibilitatea si cerințele de implementare. Aceasta evaluare va include identificarea dispozitivelor care vor fi integrate cu soluția ofertata si nivelurile de control necesare.

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 27.11.2025

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIE
NUMĂR 272 / 11.11.2025

	• Identificarea politicilor de acces: Se definesc politicile de acces in funcție de tipul de utilizatori (angajați, contractori, oaspeți) si dispozitive (corporative sau BYOD).
8.2	**Instalarea si configurarea aplicației** • Instalarea mașini virtuale: Se configurează si instalează mașină virtuala in infrastructura Beneficiarului • Configurarea bazei de date de utilizatori: Aplicația se va integra cu Active Directory pentru a centraliza autentificarea.
8.3	**Integrarea cu infrastructura existenta** • Configurarea echipamentelor de rețea: Se va configura un pilot de 2 echipamente din rețea pentru a permite autentificarea si autorizarea utilizatorilor si dispozitivelor prin aplicația solicitata, folosind protocoale precum 802.1X, MAB (MAC Authentication Bypass), sau WebAuth. Restul de echipamente din rețea se vor configura de către Beneficiar pe baza unui template pus la dispoziție de Ofertant.
8.4	**Definirea si implementarea politicilor de acces** • Crearea politicilor de acces si control: Ofertantul va configura politici de acces pe baza identității utilizatorilor, rolurilor acestora si tipului de dispozitiv.
8.5	**Testarea si optimizarea politicilor** • Testarea accesului utilizatorilor si dispozitivelor: Se efectuează teste pentru a verifica daca politicile de acces funcționează corect si daca utilizatorii si dispozitivele sunt clasificate si autorizate corect. • Optimizarea si ajustarea politicilor: Pe baza testelor si a feedback-ului, Ofertantul va ajusta politicile de acces pentru a îmbunătăți performanta si securitatea rețelei.
8.6	**Documentare** • Ofertantul va documenta procesul de implementare, configurările efectuate si procedurile pentru utilizarea si administrarea soluției propuse. • Ofertantul va elabora un document de arhitectura care sa cuprindă: descrierea sistemului, descrierea tehnologiilor utilizate si configurațiile, modul de integrare si interconectare al elementelor componente.
8.7	**Training pentru echipa de operațiuni a Beneficiarului** • Ofertantul va oferi un training de tip Knowledge Transfer pentru echipa Beneficiarului responsabila de operarea si monitorizarea soluției. • Trainingul va acoperi minim următoarele: - Utilizarea tabloului de bord si a rapoartelor - Configurarea si gestionarea politicilor de acces - Autentificare si autorizare (AAA) - Detectarea si remedierea incidentelor - Gestionarea certificatelor si a securității de rețea - Roluri și permisiuni - Actualizări si patch-uri.

ANEXA nr. 7 - CERINȚE TEHNICE *FIREWALL WAN*

Firewall WAN - se va livra 1 bucată și va avea următoarele specificații tehnice:

1. Cerințe generale ale soluției	
1.1	Echipament de tip hardware dedicat
1.2	Funcții de securitate NGFW, RAVPN, IDS/IPS, senzor Netflow, Antimalware
1.3	Funcționare in mod activ/pasiv HA
1.4	Integrare cu soluții de colectare de telemetrie Netflow
1.5	Integrare cu soluții de autentificare, autorizare si accounting Radius
1.6	Integrare cu soluții de autentificare multifactor prin SAML
1.7	Integrare cu arhitectura Secure Access Service Edge (SASE)
2. Certificări și garanții de autenticitate hardware și software	
2.1	Echipamentul va deține mecanisme de protecție împotriva alterării, înlocuirii sau intervențiilor neautorizate asupra software-ului ce rulează pe echipament.
2.2	Semnare criptografică a software-ului de producător, lansarea în execuție controlată (secure boot).
2.3	Chip TPM (trusted platform module) instalat pentru identificarea platformei hardware unic și autentic.
2.4	Verificări combinate prin care software-ul semnat criptografic este lansat pe platforma hardware destinat acestuia.
2.5	Compliant cu directivele europene 2004/108/EC si 2006/108/EC
2.6	Sistem de operare dedicat si securizat, fără utilizarea sistemelor de operare de uz general
3. Necesar minim de interfețe de interconectare, performante hardware și accesorii de instalare	
3.1	Porturi 8 x 10/100/1000 1000BASE-T si 4 x SFP+ 1/10Gbps Ethernet
3.2	Performanta Firewall: 18 Gbps (cu pachete de 1024B)
3.3	Performanta Firewall si IPS/IDS: 12 Gbps (cu pachete de 1024B)
3.4	Performanta NGFW: 12 Gbps
3.5	Performanta decriptare TLS: 3,2 Gbps măsurata cu cifru AES256 si RSA2048
3.6	Sesiuni concurente: 600.000, cu detecția aplicațiilor procesate (AVC)
3.7	Conexiuni noi pe sec: 70.000 cu detecția aplicațiilor procesate (AVC)
3.8	Throughput IPSec VPN: 18Gbps
3.9	Stocare software si loguri: minim 450GB SSD
3.10	Stabilire a 1000 de conexiuni VPN simultan, de tip RA VPN sau site-to-site VPN
3.11	Inspecție IDS/IPS: 12 Gbps, cu detecție și control la nivel de aplicație
3.13	Moduri de configurare concurenta a interfețelor: L2 bridge, L3 routed/NAT, pereche inline cu captura pasiva pentru analiza IDS, portchannel/etherchannel 802.3ad
3.14	Domenii virtuale de rutare: 10
3.15	Accesorii incluse pentru instalarea în rack de telecomunicații cu lățimea de 19" si înălțimea de 1RU standard EIA-310-D
3.16	Sursa alimentare si cablu de alimentare incluse, tensiune de alimentare 110-240V, frecventa 50-60Hz, standard EU.
4. Funcții de Firewall și NGFW incluse și licentiate	

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 13.11.2025

4.1	Funcții de NAT, object-based NAT și twice-nat, FQDN NAT
4.2	Funcții de utilizare zone de securitate cu asocierea mai multor interfețe sau subinterfete unei zone de securitate
4.3	Funcții de rutare: protocoale de rutare RIP, OSPF, BGP, BGPv6, ECMP, ISIS, EIGRP sau echivalent compatibil, VXLAN, BGP-BFD
4.4	Funcții de integrare in arhitectura SASE: PolicyBased routing cu monitorizarea metricilor RTT, Jitter si packet-loss, monitorizare interfețe prin IPSLA, configurarea aplicațiilor ce se vor ruta prin Direct Internet Access (DIA)
4.5	Funcții de context-aware firewall și identity-based firewall în concordanță cu sistemul de management al utilizatorilor
4.6	Funcții de context-aware firewall cu telemetrie XMPP conform RFC 8600 sau API WebSockets
4.7	Servicii de autentificare-autorizare-accounting (AAA) folosind minim următoarele protocoale: LDAP, RADIUS, SAML
4.8	Funcții de redundanta active-standby pentru tunele IPSec site2site
4.9	Funcții de definire interfețe tunel virtuale VTI
4.10	Funcții de remote acess VPN IPSec si TLS cu suport pentru autentificarea prin SAML si certificate digitale
4.11	Funcții de configurare pentru Remote access fără parola (passwordless) prin autentificări alternative folosind protocoale WebAuthN, FIDO, SSO si U2F
4.12	Suport pentru protocol IKEv2, cu suite de criptare cu AES-GCM, AES-GMAC cu chei de minim 256biti, algoritmi de hashing SHA-384, SHA-512, schimb de chei folosind algoritm cu curbe eliptice ECDH-256
4.13	Suport pentru Network Virtualization Encapsulation L2 protocol (GENEVE)
4.14	Funcții de configurare zone de securitate si segmentare intre zone de securitate, fiecare zona de securitate fiind aplicabila pe interfețe si sub-interfețe virtuale
4.15	Export de telemetrie Netflow către un colector dedicat pentru analiza in amănunt a pachetelor tranzitate
4.16	Decriptare și inspecție a traficului TLS, cu posibilități de a decripta cu certificat si cheie cunoscute si certificat ce resemnează sesiunea decriptata, pentru variantele TLS1.1, TLS1.2 si TLS1.3
4.17	Decriptarea TLS va tine cont prin configurare, de detaliile certificatelor expuse de servere daca: sunt selfsigned, expirate, invalide, cu lista de revocare invalida, cu domenii web ce nu corespund serverului ce prezinta certificatul, revocate sau cu emitent invalid
4.18	Funcții de inspecție a neconformităților certificatelor TLS prezentate de server si va permite blocarea sesiunilor TLS către acestea fără sa mai decripteze; Echipamentul va tine cont de tipul de cifruri minim permis, punând la dispoziția operatorului lista de cifruri permise, apoi blocând conexiuni TLS cu servere ce încearcă sa negocieze cifruri vechi si vulnerabile
4.19	Funcții de blocare a traficului HTTP/3 advertisement
4.20	Funcții de inspecție si blocare a comunicațiilor ce necesita numele serverului criptat (ESNI encrypted Server Name Identification)
4.21	Funcții de vizibilitate si amprentare a traficului criptat fără ca acesta sa necesite decriptare, degrevând astfel încărcarea echipamentului; Vizibilitatea va include protocoalele noi TLS1.2, TLS1.3 si QUIC
5.	**Functii de IPS/IDS si detectie de aplicatii incluse si licentiate**

5.1	Funcții de IPS/IDS, cu posibilități incluse de scriere reguli IPS/IDS personalizate, în format compatibil cu regulile de compunere open-source IPS/IDS snort
5.2	Funcția de IPS va asigura si inspecție preliminara a unui flux de date, dacă fluxul de date este conform cu politica de acces, dacă sursa și destinația sunt de încredere, dacă protocolul este cel desemnat, dacă banda acestuia crește peste un anumit prag, fluxul să fie redirecționat direct, fără inspecție IPS ulterioara
5.3	Funcția de IPS va permite acțiuni de eliminare a unui pachet de date detectat in traficul inspectat, prin care se elimina amenințarea si nu se resetează sesiunea către aplicații
	Funcția de IPS va permite acțiuni de rescriere a unui pachet de date detectat in traficul inspectat, prin care se elimina amenințarea si nu necesita retransmisii iar sesiunea către aplicații este nealterata
5.4	Flux de telemetrie furnizat si actualizat automat de producător, prin care echipamentul este înștiințat periodic de destinații din internet ce sunt deja cunoscute ca fiind rău intenționate si care sunt catalogate într-o lista neagra generala, cu subdiviziuni pe categorii de impact cum ar fi "Atacatori", "Bots", CnC", "Exploit", "ToR" si altele. Daca traficul supus inspecției are ca sursa sau destinație una din aceste destinații din lista neagra, atunci echipamentul trebuie sa blocheze accesul in mod prioritar, fără sa mai proceseze traficul pe alte reguli mai explicite si de content filtering, degrevând încărcarea echipamentului
5.5	Funcții de catalogare a traficului care-l tranzitează și să-l asocieze unei liste de aplicații cunoscute și actualizate de producător. Catalogarea traficului va fi raportat în sistemul de management; Minimul de aplicații detectabile si instalate in echipament la momentul punerii in funcțiune va fi de 4000
5.6	Detecția aplicațiilor detectate in traficul procesat si controlul acestora, cu mecanism de definire si dezvoltare de semnături pentru aplicații noi si proprietare in mod autonom si fără intervenția producătorilor
5.7	Protecție anti-DoS/DDoS prin blocarea atacurilor de tip SYN-Flood, ICMP-Flood și prin limitarea din regulile IPS a numărului de conexiuni către anumite resurse
5.8	Exportul logurilor IPS/IDS in format JSON de generație noua
5.9	Funcții de detecție a tiparelor de trafic foarte lungi si cu dimensiune mare (elephant flows) ce pot impact echipamentul
5.10	Funcții de extracție si inspecție a macro VBA din documente Microsoft Office
5.11	Funcții de inspecție si normalizare JavaScript si JIT (just-in-time) inspection
5.12	Funcții de inspecție SMB3 pentru Scale-Out, Directory Leasing si Multichannel
6. Funcții de Antimalware și sandbox incluse și licentiate	
6.1	Funcții de detecție și protecție antivirus și anti malware pentru fișierele care-l tranzitează; Inspecția, detecția și verdictul analizei unui fișier să se facă prin procese interne sau cu ajutorul unui serviciu specializat, furnizat de producător.
6.2	Funcție de menținere a confidențialității fișierelor inspectate, să nu necesite metode de exportare a fișierelor sau conținutului acestora din echipament în timpul inspecției. Dacă pentru obținerea fișierului este necesară interogarea serviciului furnizat de producător, se cere să se utilizeze mecanisme de amprentare unică și de anonimizare a fișierelor conform SHA256.
6.3	Funcții de a capta si trimite fișiere suspicioase, către analiza "Sandbox", iar raportul analizei, scorul asociat și indicatorii de risc se raportează platformei de management, in mod automat.

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 / 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

6.4	Trimiterea fișierelor pentru analiza în "Sandbox", trebuie să fie la latitudinea operatorului, nu automat. De asemenea, operatorul trebuie să poată configura ce tipuri de fișiere sunt foarte riscante (exe, dll, scr) iar acestea să poată fi trimise automat, în timp ce alte tipuri de fișiere, să fie doar scanate, captate dar nu trimise.
6.5	Funcții de analiza in adâncime si ML (machine learning) prin care se reverifica in mod constant postura unui fișier inspectat, pe perioada îndelungata si poate reveni asupra posturii acestuia daca aceasta se schimba (analiza retrospectiva).
6.6	Funcții de antivirus local pe echipament, ce poate fi configurat selectiv pentru anumite extensii de fișiere specifice.
	7. Funcții de Web și Content filtering licentiate ulterior
7.1	Detecție si catalogare a conținutului web HTTP si HTTPS, apoi redirectarea acestuia prin protocol WCCP către un echipament opțional specializat de filtrare URL si Web din cadrul perimetrului; echipamentul va menține funcția sa de inspecție TLS descrisa mai sus, pentru comunicațiile care nu folosesc porturi standard HTTP si HTTPS si pentru aplicațiile sau comunicațiile ce nu pot implementa funcția de web proxy
7.2	Funcții de filtrare a conținutului web ce are ca destinație internetul public, filtrarea făcându-se local sau printr-un serviciu specializat furnizat de producător; Funcția de filtrare web va tine cont de reputația actualizata a site-urilor vizitate, nu doar filtrare prin blacklist. Actualizarea reputației va trebui realizata de algoritmul intern al echipamentului sau de actualizarea acesteia de către producător într-un mod regulat sau când se detectează deteriorarea iminenta a reputației. Nu se intenționează administrarea locala de către client a reputației site-urilor sau a listei de site-uri blocate.
7.3	Funcții de integrare si interogare securizata a serviciului de DNS, folosind DNSCrypt
7.4	Funcții de integrare cu platforma Secure Access Service Edge (SASE) prin redirecționarea traficului destinat internetului, către o filtrare a conținutului ulterioara si suplimentara
	8.Cerinte de administrare, logare si control de la distanta
8.1	Aplicație de management locala accesibilă prin http/https, fără limitări de sistem de operare ce o pot accesa. Aplicația captează, corelează și afișează în rapoarte evenimentele detectate de echipament și trebuie să permită configurarea unitară a politicilor de securitate pe toate echipamentele din cadrul soluției.
8.2	Sa suporte asocierea către **Cisco FMC existenta în infrastructura beneficiarului**, de la același producător pentru operarea întregii configurații si funcționalități cerute, nefiind acceptate configurări alternative pe porturile de management ale echipamentului, sau prin tunele ssh, odată ce echipamentele au fost puse in funcțiune si înrolate in **FMC** Astfel, echipamentul va fi complet administrat, configurat, monitorizat, actualizat de la **FMC**. Actualizările centralizate vor include: versiuni de software, versiuni de semnături de IPS, versiuni de aplicații, patch-uri, semnături de antivirus, antimalware, fluxuri personalizate de destinații periculoase, asocieri de IP către geolocalizare.
8.3	Port USB Type-C si port serial pentru administrarea locală cat și un port 1000BASE-T dedicat exclusiv pentru management OOB. Echipamentul va fi livrat cu cablu de consola USB-C.
8.4	Administrare de la distanță prin SSH v2 cu mecanisme de criptare actualizate conform recomandărilor NIST2020, AES128, SHA256/512, KMAC128
8.5	Mecanism de verificare a unei configurații aplicate sub forma unui simulator de pachete, care sa evidențieze toate procesele pe care le efectuează echipamentul in procesarea acelui pachet simulat

AVIZAT TEHNIC
DIRECȚIA COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
NUMĂR 272 DATA 11.11.2025

MINISTERUL AFACERILOR INTERNE
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura ..... Data 25.11.2025

8.6	Mecanism de captura de trafic de la distanta, in format .pcap, exportabil direct din consola de administrare
8.7	Mecanism de replay a capturii de trafic .pcap prin echipament, pentru verificarea regulilor configurate si semnăturilor IPS/IDS active
9. Licențiere și perioada de garanție	
9.1	Telemetria de securitate si licențele necesare pentru o perioada de minim 3 ani pentru îndeplinirea funcționalităților solicitate mai sus.
9.2	Suport hardware cu SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, 24 ore timp de remediere), pe o perioadă de 3 (trei) ani, care să garanteze diagnosticarea echipamentului/modulului defect și înlocuirea acestuia, fără costuri suplimentare pentru beneficiar
9.3	Suport software pe o perioadă de 3 (trei) ani, acoperind dreptul de a face update –uri software la sistemul de operare al switch-ului ori de câte ori este necesar
9.4	Pentru suportul hardware/software se va asigura pe toata durata garanției accesul direct al beneficiarului la site-ul ofertantului cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate precum și dreptul de a face update-uri și upgrade-uri la toate componentele software (sistem de operare, firmware etc.) ori de câte ori este necesar.
9.5	In cazul in care anumite licențe sunt de tip subscripție, acestea vor fi oferite pe o perioada cel puțin egala cu durata garanției.
9.6	Se vor preciza part-number-ul (–ele) care asigura condițiile de garanție hardware si suport software mai sus menționate.