№	Specificarea tehnică deplină solicitată	Specificarea tehnică FortiNet
Cerințe tehnice		
1	Protecția rețelei cu controlul stării sesiunilor;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/hardware-acceleration/765824/np7-and-np7lite-acceleration
2	Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/954635/getting-started
3	Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP.	Compliant, https://trust.fortinet.com/
4	Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/213498/signature-based-defense
5	Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/929997/ssl-ssh-inspection
6	Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/605065/configuring-handling-of-unknown-content-types
7	Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea).	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/954635/getting-started
8	Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/hardware-acceleration/765824/np7-and-np7lite-acceleration
9	Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/hardware-acceleration/765824/np7-and-np7lite-acceleration
10	Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere.	Partial compliant, poate fi interzisa downloadarea de fisiere, identificarea account-ului personal/business, logarea in facebook. https://www.fortiguard.com/appcontrol/38517
11	Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/8049/restricted-saas-access https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/302748/application-control https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/833698/web-filter
12	Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele.	Compliant, FortiOS pe toate platformele Fortinet
13	Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/849640/credential-phishing-prevention
14	Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/419391/applying-multi-factor-authentication
15	Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/302748/application-control
16	Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe.	Compliant, odata incarcate in sistemul de operare, signaturile nu au nevoie de access la internet. https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/408891/ai-and-ml-based-ips-detection
17	Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații:	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.1 .	Aplicații corporative:	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.1.1.	Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/622284/user-authentication
17.1.2.	Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.1.3.	Servicii de fișiere, inclusiv Microsoft SMB.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/186160/cifs-support
17.1.4.	ERP, CRM, inclusiv SAP, 1C;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.1.5.	Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus;	Test
17.1.6.	Protocoale de schimb de e-mail: SMTP, POP3, IMAP;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/673670/protocols-and-actions
17.1.7.	Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/858887/voip-solutions
17.1.8.	Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/785428/isdb-fqdn-groups
17.1.9.	Servicii de backup, inclusiv Symantec Backup Exec;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/785428/isdb-fqdn-groups
17.1.10.	Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol
17.1.11.	Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol
17.1.12.	Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol
17.1.13.	Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN;	Compliant, SSL vpn supportat in software versiunea <7.4.8, IPSec (including PQC - criptarea quantica) suporatate pe toate modelele si softurile curente

17.2.	Aplicații Internet:	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.1.	E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.2.	Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/419391/applying-authentication
17.2.3.	Servicii de mesagerie instantanee, inclusiv Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.4.	Servicii de conferință audio-video	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/419391/applying-authentication
17.2.5.	Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, WebDav;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.6.	Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.7.	Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.8.	Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
17.2.9.	Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
18	Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodoare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/233445/blocking-applications-with-custom-signatures
19	Recunoașterea aplicațiilor transmise prin protocolul HTTP/2;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/710924/http-2-support-in-proxy-mode-ssl-inspection
20	Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/122078/deep-inspection https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/430005/certificates
21	Inspecția tunelurilor:	
21.1.	Generic Routing Encapsulation (GRE) (RFC 2784);	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/250464/cisco-gre-over-ipsec-vpn
21.2.	Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)];	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/484445/fortigate-encryption-algorithm-cipher-suites
21.3.	Mod de transport AH IPSec.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/790613/phase-1-configuration
22	Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/hardware-acceleration/765824/np7-and-np7lite-acceleration
23	Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/934626/captive-portals
24	Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virușilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
25	Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune:	
25.1.	Adresa IP a expeditorului,	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
25.2.	Adresa IP a destinatarului,	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
25.3.	Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP,	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
25.4.	Numele utilizatorilor sau grupurilor de utilizatori din Active Directory,	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
25.5.	Aplicațiile la nivelul 7 al modelului OSI,	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
25.6.	URL categorii.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy

26	Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni:	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
	• Permisiune sau interdicție;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
	• Permisiunea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de interacțiuni;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
	• Permisiune, dar cu scanare pentru viruși și alte amenințări;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
	• Permisiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
	• Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/929997/ssl-ssh-inspection
	• Ne-decriptarea anumitor categorii de URL și site-uri web de încredere;	Compliant, SSL excempt, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/929997/ssl-ssh-inspection
	• Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/297431/traffic-shaping
	• Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/297431/traffic-shaping
	• Aplicarea redirecționării traficului pe bază de politici (Policy Based Forwarding);	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/144044/policy-routes
	• Permisiunea anumitor funcții ale aplicației;	Compliant
	• Oricare combinație dintre acțiunile de mai sus.	Compliant
27	Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
28	Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/605065/configuring-handling-of-unknown-content-types
29	Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
30	Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/656084/firewall-policy
31	Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări;	Compliant, Lista de aplicatii: https://www.fortiguard.com/services/appcontrol https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/019814/basic-category-filters-and-overrides
32	Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
33	Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS);	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
34	Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
35	Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
36	Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări;	
37	Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/680955/security-profiles
38	Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
39	Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2007, 2010, 2016 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
40	Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
41	Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
42	Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
43	Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
44	Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
45	Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
46	Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
47	Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
48	Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
49	Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

50	Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
51	Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
52	Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
53	Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare;	Compliant, folosind tehnici de anti-evasion (denumirea Fortinet pentru functionalitatea solicitata) https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
54	Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
55	Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament;	Partial compliant, solutia Sandbox este oferita ca service si la expirarea abonamentului are o perioada de gratie
56	Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare):Duo,	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/499536/agentless-vpn-with-okta-as-saml-idp https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/109964/agentless-vpn-with-microsoft-entra-sso-integration ,
	• Okta,	
	• RSA SecureID,	
	• PingID;	
57	Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA);	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/419391/applying-multi-factor-authentication
58	Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile;	Compliant, prin FortiClient EMS ZTNA edition, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/forticlient.pdf
59	Funcționalitate de protecție împotriva atacurilor DoS;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/771644/dos-policy
60	Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța;	Compliant, in conditiile de testare din datasheet https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
61	Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/771644/dos-policy
62	Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/83908/block-https-downloads-of-exe-files-and-log-https-downloads-of-files-larger-than-500-kb
63	Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/882673/configuring-a-file-filter-profile
64	Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/338478/advanced-dlp-configurations
65	Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/882673/configuring-a-file-filter-profile
66	Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor.	Compliant, prin FortiManager, https://docs.fortinet.com/document/fortimanager/8.0.0/upgrade-guide/262607/upgrading-fortimanager-firmware
67	Cerințe pentru sistemul de management centralizat:	
	• Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL);	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete;	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
	• Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing);	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
68	Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/103514
69	Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/697110/mirroring-ssl-traffic-in-policies
70	Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet.	Partial compliant, doar pe port extern
71	Prezența unui raport separat pentru aplicațiile de tip SaaS.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
72	Funcționalitatea IPSec VPN.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/520377/ipsec-vpn
73	Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/250999/log-settings-and-targets

74	Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/479509/dynamic-routing
75	Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3).	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/302871/transparent-mode
76	Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
77	Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/999756/multicast
78	Suport pentru rutarea între VLAN-uri.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
79	Suport pentru NAT, DHCP și DHCP relay.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/783526/dhcp-servers-and-relays
80	Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri).	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/402940/vlan
81	Suport pentru agregarea interfețelor prin 802.3ad (suport LACP).	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/567758/aggregation-and-redundancy
82	Suport pentru pachete mari (Jumbo frames).	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/596096/interface-mtu-packet-size
83	Managementul rolurilor administratorilor locali:	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/294491/administrator-profiles
	• Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte);	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/109991/virtual-domains
	• Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web;	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/109991/virtual-domains https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/294491/administrator-profiles
	• Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/109991/virtual-domains https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/294491/administrator-profiles
84	Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului.	Compliant, https://docs.fortinet.com/document/fortigate/8.0.0/hardware-acceleration/575471/network-processors-np7-np7lite-np6-np6xlite-and-np6lite
	Cerințe de performanță ale firewall-ului:	
	Performance:	
	• Threat prevention throughput 1.2 Gbps;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• IPsec VPN throughput 800 Mbps;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Connections per second 1100;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Firewall throughput 1.4 Gbps;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Policies:	
	• Security rules min 500;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Security rule schedules min 256;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• NAT rules min 400;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Tunnel content inspection rules 100;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• SD-WAN rules min 100;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Policy based forwarding rules min 100;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• DoS protection rules min 100.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Security Zones:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• security zones 25.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Security Profiles:	
	• Security profiles min 75.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	URL Filtering:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Total entries for allow list, block list and custom categories 25,000;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Interfaces:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• I/O: 1G RJ45 (7);	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (1).	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Storage Capacity:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• 128 GB	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf + 64GB USB3.1 Flash Drive
	Virtual Routers:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Virtual routers 3.	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Routing:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• IPv4 forwarding table size min 5,000;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• IPv6 forwarding table size min 2500;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• System total forwarding table size min 5,000;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	L2 Forwarding:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• ARP table size per device 1500;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• IPv6 neighbor table size 1500;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• MAC table size per device 1500;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	Address Assignment:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• DHCP servers 3;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf

	• DHCP relays 500;	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	IPSec VPN:	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• Suport Site to site over gre IPSec tunnels	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
	• SD-WAN IPsec tunnels	Compliant, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-70g-series.pdf
85	Alte cerințe obligatorii:	
	- Garanție, Mentenanta si Suport HW+SW incluse – 12 luni;	Compliant
	- Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului;	Compliant
	- Ofertantul va indica în ofertă costul serviciilor pentru efectuarea instalării și configurării a echipamentului ofertat, va asigura integrarea echipamentului ofertat cu dispozitivele existente pe baza platformei existente in cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului.	Compliant
	- Prezentarea a certificatelor a minim 1 specialist pe produsul ofertat din partea ofertantului (fără asociere cu o alta companie);	Compliant
	- Ofertantul va prezenta copia Certificatului ISO 27001:2018, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT	Compliant
	- Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware si software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea si managementul infrastructurii IT si de Securitate – certificat confirmat cu aplicarea semnăturii electronice;	Compliant
	- Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa;	Compliant
	- Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013;	Compliant
	- Referințe de vânzare NGFW – minim 3 contracte;	Compliant
	- Termen de livrare: maxim pana la 90 zile de la data intrării în vigoare a contractului	Compliant