

Specificații tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziție ocds-b3wdp1-MD-1784119650788 din 15.07.2026
Obiectul achiziției: Echipamente de rețea de tip Next Generation Firewall (NGFW)

Denumirea bunurilor	Denumirea modelului bunului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Echipamente de rețea de tip Next Generation Firewall (NGFW)						
<i>Echipamente de rețea de tip Next Generation Firewall (NGFW)</i>	PAN-PA-510 Palo Alto Networks PA-510	USA	Palo Alto Networks, Inc.	Conform cerintelor din Anuntul de participare	Conform Matricei de conformitate, Apendice la Anexa 22.	

Semnat:

Nume: **Irina Vicol**

În calitate de: **Administrator**

Ofertantul: **Xontech Systems SRL**

Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

Matricea de conformitate conform caietului de sarcini solicitate in SIA RSAP si documentatia standard

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
1.	Echipamente de rețea de tip Next Generation Firewall (NGFW)	Echipamente de rețea de tip Next Generation Firewall (NGFW) Cerințe tehnice - Protecția rețelei cu controlul stării sesiunilor; - 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; - 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. - Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. - Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. - Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. - 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). - Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o	Se ofera echipamentul NGFW PAN-PA-510 Palo Alto Networks cu inspecție la Layer 7 ce va conține modulele de securitate cu mentenanța și suport pentru 12 luni incluse așa ca: (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), inclusiv va veni în set cu accesorii pentru montare în dulap de tip rack. Firewall-ul oferat va acoperi toate specificațiile tehnice menționate mai jos: - Protecția rețelei cu controlul stării sesiunilor; - 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; - Firewall-ul NGFW propus este certificat conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. - Firewall-ul NGFW propus nu necesita o repornire pentru a verifica și instala actualizările de securitate. - Firewall-ul NGFW identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. - Firewall-ul NGFW clasifica aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. - Firewall-ul NGFW e o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). - Firewall-ul NGFW este dezvoltat inițial cu o arhitectură de procesare paralelă a

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

	arhitectură de procesare paralelă a traficului pe un singur pas. 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 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. 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1. Aplicații corporative: 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 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; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225,	traficului pe un singur pas. 9. Firewall-ul NGFW este dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 10. Firewall-ul NGFW delimitează diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. 11. Firewall-ul NGFW controlează accesul aplica politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW utilizează un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW sprijină crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW sprijină aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW permite vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW oferă algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1. Aplicații corporative: 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 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; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225,
--	---	--

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

	Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv ICQ, Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video, inclusiv Skype; 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, SkyDrive, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 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; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 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	Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv ICQ, Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video, inclusiv Skype; 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, SkyDrive, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 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; 18. Oferă instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoaște aplicații transmise prin protocolul HTTP/2; 20. Recunoaște aplicații 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,
--	---	---

	aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; 21.3. Mod de transport AH IPSec 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 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; 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 virusilor 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; 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, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 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	inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; 21.3. Mod de transport AH IPSec 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 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; 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 virusilor 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; 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, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 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
--	---	---

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

	existe posibilitatea implementării următoarelor acțiuni: • Permise sau interdicție; • Permisele 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; • Permise, dar cu scanare pentru viruși și alte amenințări; • Permise sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interdicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirectionării traficului pe bază de politici (Policy Based Forwarding); • Permisele anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 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; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat;	existe posibilitatea implementării următoarelor acțiuni: • Permise sau interdicție; • Permisele 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; • Permise, dar cu scanare pentru viruși și alte amenințări; • Permise sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interdicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirectionării traficului pe bază de politici (Policy Based Forwarding); • Permisele anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 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; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL este realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analizează SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat;
--	---	---

	33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 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; 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; 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; 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; 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2003, 2007 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 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; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 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; 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; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului;	33. Analizează cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detecta tehnici 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; 35. Blocheaza domenii 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; 36. Analizeaza cereri 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; 38. Oferă 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; 39. Sandbox-ul verifică fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2003, 2007 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 40. Firewall-ul trimite spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; 41. Sandbox-ul generează și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul generează 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; 43. Firewall-ul primește semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud are posibilitatea de a schimba semnături între toți clienții furnizorului;
--	---	--

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

	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. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 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; 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; 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; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare; 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; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament;	45. Firewall-ul primește din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul verifică linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul verifică fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Oferă suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul asigura 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; 50. Integrări 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; 51. Sandbox-ul local dedicat are un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul generează rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud utilizează tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare; 54. Firewall-ul are 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; 55. Sandbox-ul cloud accepta fișiere PE pentru verificare, chiar și în absența unui abonament;
--	---	--

	56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare): Duo, • 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); 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; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; 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; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 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.;	56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare): Duo, • 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); 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; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibil de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcțional de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectează obiecte din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; 63. Detectează prezența 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; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibil de integrat cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 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.;
--	--	--

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

	• 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); • 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; • 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. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Platforma trebuie să suporte gestionarea a cel puțin 1000 de echipamente firewall de nouă generație (NGFW); • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN.	• 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); • Posibil de corelat automat evenimentele 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; • 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. • Posibil de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Platforma suporta gestionarea a cel puțin 1000 de echipamente firewall de nouă generație (NGFW); • Sistemul poate exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Există mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • E posibil actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția oferă interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator poate face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul permite definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma permite organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul suporta funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibil de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN.
--	--	---

	73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 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.	73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibil de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibil de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibil de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware dispune de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Asigura resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte 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) este unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului.
--	--	---

	Cerințe de performanță ale firewall-ului: Performance: • Threat prevention throughput 1.2 Gbps; • IPsec VPN throughput 800 Mbps; • Connections per second 1100; • Firewall throughput 1.4 Gbps; Policies: • Security rules 500; • Security rule schedules 256; • NAT rules 400; • Tunnel content inspection rules 100; • SD-WAN rules 100; • Policy based forwarding rules 100; • Captive portal rules 10; • DoS protection rules 100. Security Zones: • Max security zones 25. Security Profiles: • Security profiles 75. URL Filtering: • Total entries for allow list, block list and custom categories 25,000; Interfaces: • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (1). Storage Capacity: • 128 GB eMMC Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size 5,000; • IPv6 forwarding table size 2500; • System total forwarding table size 5,000;	Caracteristici de performanță ale firewall-ului: Performance: • Threat prevention throughput 1.2 Gbps; • IPsec VPN throughput 800 Mbps; • Connections per second 1500; • Firewall throughput 1.8 Gbps; Policies: • Security rules 750; • Security rule schedules 256; • NAT rules 400; • Tunnel content inspection rules 100; • SD-WAN rules 100; • Policy based forwarding rules 100; • Captive portal rules 10; • DoS protection rules 100. Security Zones: • Max security zones 50. Security Profiles: • Security profiles 60. URL Filtering: • Total entries for allow list, block list and custom categories 25,000; Interfaces: • I/O: 1G RJ45 (8); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2). Storage Capacity: • 128 GB eMMC Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size 5,000; • IPv6 forwarding table size 2500; • System total forwarding table size 5,000;
--	---	--

	L2 Forwarding: • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; Address Assignment: • DHCP servers 3; • DHCP relays 500; IPSec VPN: • Suport Site to site over gre IPSec tunnels • SD-WAN IPsec tunnels 85. Alte cerințe obligatorii: - Garanție, Mentenanta si Suport HW+SW incluse – 12 luni; - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului; - 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 în cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului. - Prezentarea a certificatelor a minim 1 specialist pe produsul ofertat din partea ofertantului (fără asociere cu o alta companie); - Ofertantul va prezenta copia Certificatului ISO 27001:2018, în domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT - 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; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa;	L2 Forwarding: • ARP table size per device 2000; • IPv6 neighbor table size 2000; • MAC table size per device 2000; Address Assignment: • DHCP servers 16; • DHCP relays 500; IPSec VPN: •Max IKE Peers1,000 •Site to site (with proxy id)1,000 •D-WAN IPSec tunnels1,000 85. Alte cerințe obligatorii: - Garanție, Mentenanta si Suport HW+SW incluse – 12 luni; - Producătorul va oferi suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea Xontech Systems SRL în calitate de partener autorizat; - Este inclus în oferta costul serviciilor pentru efectuarea instalării și configurării a echipamentului ofertat, va asigura integrarea echipamentului ofertat cu dispozitivele existente pe baza platformei existente în cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului. - Certificatele a minim 1 specialist pe produsul ofertat din partea Xontech Systems SRL anexate cu oferta (fără asociere cu o alta companie); - Certificatul ISO 27001:2018, în domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT este anexat cu oferta; - Certificatul 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 anexat cu oferta si confirmat cu aplicarea semnăturii electronice; - Autorizarea de la producător pentru licitația la care participa este anexat cu oferta;
--	---	--

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001

		- Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; - Referințe de vânzare NGFW – minim 3 contracte; - Termen de livrare: maxim pana la 90 zile de la data intrării în vigoare a contractului	- O persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013 – certificat anexat cu oferta; - Xontech Systems SRL detine Referințe de vânzare NGFW – minim 3 contracte - la solicitare se va prezenta documentele confirmative; - Termen de livrare: maxim pana la 90 zile de la data intrării în vigoare a contractului Detalii tehnice suplimentare in datasheet anexat cu oferta sau linkul de mai jos: https://www.paloaltonetworks.com/products/product-selection#:~:text=Compare-,PA-510
--	--	--	--

Configuratia ofertata si descrisa mai sus:

Product Code	Description	Product Type	Qty
PAN-PA-510	Palo Alto Networks PA-510	Hardware	10
PAN-1RU-4POST-RACK-10	1RU 4-Post rack mount for: two PA-510s and four power adapters, one PA-505 and one power adapter	Hardware	10
PAN-PA-510-BND-PRECISIONAI	PA-510, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 year (12 months) term	License	10
PAN-SVC-BKLN-510	PA-510, Partner enabled premium support, 1 year (12 months) term.	Support	10

S.C. "XONTECH Systems" S.R.L.
IDNO: 1018600044509, TVA: 0610683
Adresa fizică: 6A, Calea Ieșilor st.,
Artima – Business & Lifestyle Center of. 210B
Republica Moldova, Chișinău, MD-2069.

B.C. MOLDOVA-AGROINDABNK S.A.,
Sucursala Stefan cel Mare
str.V. Alecsandri 115, Chisinau, R.M.
Swift: AGRNMD2X
IBAN: MD40AG000000022515173001