Anexa nr.1
la Caietul de sarcini

Specificaţii tehnice

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

Numărul procedurii de achiziţie:	ocds-b3wdp1-MD-1654178592543 din 17 iunie 2022
Denumirea procedurii de achiziţie:	**Soluții de securitate antispam, WAF și proxy**

Denumirea bunurilor	**Denumirea modelului**	**Ţara de origine**	**Produ-cătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standar de de referinţă**
1	2	3	4	5	6	7
Lotul 2: Soluție virtuală de tip Web Application Firewall						
Soluție virtuală de tip Web Application Firewall	**Part Number** / **Description** / **Qty**: F5-BT-200MBUNDLE — BIG-IP: VE Subscription 200M Best Bundle — 2 F5-ADDIPI200MPRMSUB — BIG-IP: VE Subscription Add IPI 200M (Premium Support) — 2 F5-ADDTC200MPRMSUB — BIG-IP: VE Subscription Add Threat Campaigns 200M (Premium Support) — 2 F5-BIG-SPT-PRM — BIG-IP: VE Subscription Premium Support — 2	**SUA**	**F5 Networks, Inc.**	Conform caietului de sarcini solicitat, mentionat in Anexa 1 la formular. Matricea de conformitate	Conform caietului de sarcini solicitat, mentionat in Anexa 1 la formular. Matricea de conformitate	

Semnat:
Nume: **Irina Vicol**
În calitate de: **Administrator**
Ofertantul: **Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.
Data:

Digitally signed by Vicol Irina
Date: 2022.06.17 16:45:58 EEST
Reason: MoldSign Signature
Location: Moldova

Anexa 1

Matricea de conformitate conform cerințelor solicitate in Anexa 1 pentru Lotul 2:

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
		Lotul 2	
1.	Soluție virtuală de tip Web Application Firewall	Tip: Soluție virtuală de tip Web Application Firewall, inclusiv 12 luni de suport și subscriere de la producător. Cerințe de licențiere: - Este responsabilitatea Ofertantului de a determina modelul de licențiere și cantitatea licențelor; - Modelul de licențiere propus trebuie să acopere 2 instanțe; - Soluția livrată va include prețul pentru 12 luni de suport și subscriere de la producătorul soluției, care va începe de la data acceptanței soluției, după instalare și testare a	Tip: Se oferă Soluție virtuală de tip Web Application Firewall, inclusiv 12 luni de suport Premium și subscriere de la producător. Soluția **F5 Best License Bundle** care include modulele LTM, DNS, AFM, APM, AWAF, IPI 200M, Threat Campaigns 200M, denumirile complete și descrierea detaliata cu funcționalitățile adiționale cerințelor solicitate sunt menționate la finalul matricei și în datasheeturile anexate cu oferta pentru fiecare modul a soluției ofertate: BIG-IP: VE Subscription Add AFM 200M (Premium Support) 2 BIG-IP Virtual Edition Add-on License for Access Policy Manager 200Mbps (500 SSLVPN) 2 BIG-IP: VE Subscription Add DNS 1000 RPS (Premium Support) 2 BIG-IP: VE Subscription LTM 200M (Premium Support) 2 BIG-IP: VE Subscription Add AWF 200M (Premium Support) 2 BIG-IP: VE Subscription Add Threat Campaigns 200M (Premium Support) 2 BIG-IP: VE Subscription Add Threat Campaigns 200M (Premium Support) 2 Descriere generală licențiere: - Se oferă Cluster a 2 instanțe BIG-IP Virtual Edition (VE) cu un trafic de 200Mbps pentru fiecare instanță. Traficul total în configurarea clusterului in modul Active-Active va fi pînă la 400Mbps. - Soluția ofertată include prețul pentru 12 luni de suport premium și subscriere de la producătorul soluției, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților.

		funcționalităților. În cazul activării licenței până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). **Cerințe generale:** • Soluția trebuie să fie propusă ca un Appliance Virtual, compatibilă cu platformele virtuale VMware vSphere 7.0 și Citrix 8.1; • Soluția trebuie să fie în configurația de High-Availability (Active-Active); • Soluția trebuie să asigure minim o performanță de procesare (HTTP) de 100 Mbps; • Modelul de licențiere nu trebuie să limiteze numărul de aplicații protejate. • **Cerințe față de funcționalitatea Application Delivery:** - URL Rewriting; - HTTPS/SSL Offloading; - HTTP Compresion; - Caching; - Layer 7 load balancing. • **Cerințe față de protecția Aplicațiilor:** - Cross Site Scripting; - Bot based; - DoS; - SQL Injection; - Session Hijacking; - Protecție împotriva OWASP top 10 atacuri; - Scanare fișiere (AV și sandbox).	Suntem de acord cu faptul că în cazul activării licenței până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Xontech Systems. **Funcționalități generale:** - Soluția se va livra ca un Appliance Virtual, compatibilă cu platformele virtuale VMware vSphere 7.0, Hyper-V Windows Server 2019, 2016,2012R2 și Citrix 7.2, 7.1, 7.0, 6.5, 6.2; - Soluția susține configurarea de High-Availability (Active-Active); - Soluția ofertată asigură o performanță de procesare (HTTP) de 200 Mbps; Traficul total în configurarea clusterului in modul Active-Active va fi pînă la 400Mbps. - Modelul de licențiere nu limitează numărul de aplicații protejate. • **Funcționalități față de Application Delivery:** - URL Rewriting; - HTTPS/SSL Offloading; - HTTP Compresion; - Caching; - Layer 4-7 load balancing. • **Funcționalități față de protecția Aplicațiilor:** - Cross Site Scripting; - Bot based; - DoS; - SQL Injection; - Session Hijacking; - Protecție împotriva OWASP top 10 atacuri;

			- Trimiterea fișierelor pentru scanare către o soluție existentă (AV și sandbox).
		• **<u>Cerințe față de serviciile de Securitate:</u>** - Detecție malware; - Protecție brute-force; - Prevenție DoS; - Protecție XML și JSON REST API; - Mecanisme de protecție bazate pe Machine Learning; - Protecție împotriva scurgerii datelor; - L4 Stateful Network Firewall; - HTTP Header Security; - Known threat and zero-day attack protection; - Data leak prevention; - Web Defacement Protection; - Geo-IP și IP Reputation.	• **<u>Funcționalități față de serviciile de Securitate:</u>** - Detecție malware; - Protecție brute-force; - Prevenție DoS; - Protecție XML și JSON REST API; - Mecanisme de protecție bazate pe Machine Learning; - Protecție împotriva scurgerii datelor; - L4 Stateful Network Firewall; *(BIG-IP AFM is a stateful, full-proxy security solution that provides advanced network protection and capabilities that exceed traditional firewalls.)* o Protocol anomaly detection (SYN /ICMP /ACK /UDP /TCP /IPv4 /IPv6 /DNS /ARP) o DoS and DDoS protection (L3, L4, SSL/TLS, HTTP, Flood, Sweep) o Remotely trigger black hole filtering (RTBH) o SSH Proxy o Port-misuse protection o SSL/TLS Reverse proxy o IP reputation and geolocations o Central management w/RBAC o SNMP reporting o DDoS traffic sampling - HTTP Header Security; - Known threat and zero-day attack protection; - Data leak prevention; - Web Defacement Protection; - Geo-IP și IP Reputation.

		• **<u>Cerințe față de mecanimsele de autentificare:</u>** - Suportul protocoalelor de autentificare SAML, LDAP, RADIUS; - Autentificarea pe bază de certificat; - Suport 2-factor authentification. • **<u>Cerințe față de Administrare și Raportare:</u>** - Interfață web de administrare; - Dashbord-uri informaționale; - Rapoarte și log-uri centralizate; - Syslog, snmp, email notificări; - Crearea conturilor de administrare pe bază de roluri; <u>Cerințe minime pentru perioada de suport și subscriere de la producător:</u> • 12 luni din data acceptanței soluției; • suport prin e-mail sau conectare de la distanță de la producător. <u>Notă:</u> După deschiderea ofertelor, pentru verificarea corespunderii soluției ofertate cu cerințele înaintate, la solicitare Ofertantul va pune la dispoziția Autorității contractante în decurs de 3 zile lucrătoare pentru testare versiunea trial a soluției ofertate. <u>Alte cerințe obligatorii:</u> Costul ofertei trebuie să includă activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe către administratorii Cumpărătorului, executate de Ofertant (Furnizor).	• **<u>Funcționalități față de mecanismele de autentificare:</u>** - Suportul protocoalelor de autentificare SAML, LDAP, RADIUS; - Autentificarea pe bază de certificat; - Suport 2-factor authentification. • **<u>Funcționalități față de Administrare și Raportare:</u>** - Interfață web de administrare; - Dashbord-uri informaționale; - Rapoarte și log-uri centralizate; - Syslog, snmp, email notificări; - Crearea conturilor de administrare pe bază de roluri; <u>Perioada de suport și subscriere de la producător:</u> • 12 luni din data acceptanței soluției; • suport prin e-mail sau conectare de la distanță de la producător. <u>Notă:</u> Suntem de acord ca după deschiderea ofertelor, pentru verificarea corespunderii soluției ofertate cu cerințele înaintate, la solicitare Xontech Systems va pune la dispoziția Autorității contractante în decurs de 3 zile lucrătoare pentru testare versiunea trial a soluției ofertate. <u>Alte cerințe obligatorii:</u> Costul ofertei include activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale) pentru 5 aplicații declarate de partea contractantă în cadrul întrebărilor de clarificare, punerea în funcțiune a soluției, precum și transferul de cunoștințe către administratorii Cumpărătorului, executate de Xontech Systems.

	Descriere Funcționalități adiționale față de cerințele solicitate pentru modulele incluse în soluția ofertată
	Se oferă Soluție virtuală de tip Web Application Firewall, inclusiv 12 luni de suport și subscriere de la producător. Soluția F5 Best License Bundle care include modulele LTM, DNS, AFM, APM, AWAF. Cluster a 2 instanțe BIG-IP Virtual Edition (VE) cu un trafic de 200Mbps pentru fiecare instanță. Traficul total în configurarea clusterului in modul Active-Active va fi pînă la 400Mbps. You will receive virtual application delivery controllers (vADCs) that can be deployed on all leading hypervisors and cloud platforms running on commodity servers. BIG-IP VEs deliver all the same market-leading Software-Defined Application Services™ (SDAS)—including advanced traffic management, acceleration, DNS, firewall, and access management. **In addition to the tender requirements**, you get the ability to balance any type of traffic tcp, udp etc. Traffic management at all levels from **L3** to **L7**. For example, creating a rule for publishing multiple applications behind the single public ip address. TCP/IP techniques and improvements in the latest RFCs with extensions to minimize the effect of congestion and packet loss and recovery. APM module in addition to access control provides remote access via SSL VPN with a secure and adaptive per-app VPN. License includes 500 concurrent SSL VPN sessions. You can even check endpoint for security compliance such as check A/V status, local Firewall status, verify if a mobile device is rooted or jailbroken, and much more. The DNS module will protect DNS from attacks as well as from DDOS. Also, this module can do global balancing for an individual application. If you have or plan to have a backup data center, it will be possible to balance traffic between data centers for each application separately. In addition to the classic DoS protection F5 offers behavioral DDoS. F5 provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. Working together with other BIG-IP DoS protections, Behavioral DoS examines traffic flowing between clients and application servers in data centers, and automatically establishes the baseline traffic/flow profiles for Layer 7 (HTTP) and Layers 3 and 4. Advanced routing enables dynamic routing such as BGP, RIP, OSPF, ISIS, BFD. As a result, you get application delivery controller that works at all levels: • DNS protection and global load balacing • AFM -L3-L4 level protection from the network attacks and DDOS

- APM Access orchestration (this includes API access as well) and SSL VPN
- AWF Application-level protection,
- LTM local load balancing

Local Traffic Manager (LTM) – Full Proxy load balancing and traffic optimization, the LTM supports a wide range of protocols and allows you to steer traffic based on just about anything you can dream up. Typically known for providing load balancing functions based on application health & performance, but the LTM can do much much more than just act as a load balancer. It can act as a reverse proxy, forward proxy, and shape/bend traffic around things like security and authentication like no other product. You can even augment client-side and server-side traffic pragmatically with iRules (client-side) and iRules LX (server-side) and is super dev-ops friendly with a full REST-based API for automation and orchestration. The LTM is also the best in the biz when it comes to terminating SSL/TLS for full HTTP traffic inspection and manipulation.

- Load balancing and monitoring
- Application visibility and monitoring
- L7 intelligent traffic management
- Core protocol optimization (HTTP, TCP, HTTP/2, SSL)
- SSL proxy and services
- IPv6 support
- Programmability (iRules®, iCall®, iControl®, iApps®)
- ScaleN™ (on-demand scaling of performance and capacity)
- BIG-IP® APM® Lite (user authentication, SSL VPN for 10 concurrent users)
- SYN flood DDoS protection

Software Services

- Advanced routing (BGP, RIP, OSPF, ISIS, BFD)

DNS - F5's DNS module provides intelligent resolution for high availability and traffic steering on a per URL basis. "Per URL", is very important to understand, because you can resolve each individual URL differently depending on the metrics you set. And again, you can do this around just about anything you can set up – i.e. health & performance monitors, GeoIP, EDNS0, you can even base availability on multiple services that make up an app, ie you can have dependency monitors to multiple endpoints to intelligently resolve the DNS request to. F5's DNS module also has full support for DNSSEC, aka the DNS Security Extensions. Lots of very large enterprises and government entities use the F5 DNS right on their edge

as their external primary authoritative name servers, largely because of the security features and the amount of requests per second it can handle. Though, it doesn't have to be authoritative, you can also implement the DNS module in a very unintrusive way utilizing CNAMES for each URL you want to intelligently resolve – makes for a nice and easy implementation.

- Global server load balancing
- DNS services
- Real-time DNSSEC solution
- Global application high availability
- Geolocation
- DNS DDoS attack prevention

Advanced Firewall Manager (AFM) – F5's AFM extends all the features of the firewall that's included in LTM and turns the BIG-IP into a firewall powerhouse. Namely, the AFM extends the logging features for denied traffic and gives you very granular control over the firewall. The AFM gives you multiple points where you can apply an ACL.

- High performance ICSA firewall
- Network DDoS protection
- Application-centric firewall policies
- Protocol anomaly detection

Access Policy Manager (APM) the APM is a swiss army knife around all things access- & authentication-related. Want to add multifactor auth (MFA) in front of an app you're pushing through the BIG-IP? How about multiple forms of auth with a decision tree based on what type of user it is (Internal, external, offshore, domestic, full browser, or thick client)? The APM makes all of that easy with its visual policy editor (VPE). There's so much you can do with the APM: Federation via SAML, OAuth, and OpenID Connect; SSO; Full SSL VPN; and even gives you the ability to host a webtop similar to something like Okta, but with far more control and visibility. APM can check A/V status, local Firewall status, verify if a mobile device is rooted or jailbroken, and much more. Need to grant secure access from the internet to an app that was never intended to be exposed to the Internet? APM has your back with portal resources. Just acquired another company and their AD is jacked up but you've been directed to merge the two? APM can help you Band-Aid that situation with some secure federation until you can properly consolidate. APM is also a great tool when you need to federate with Azure AD and provide hybrid auth between your org and the cloud. Transforming auth is a cakewalk for APM, including complicated auth like Kerberos. Still, using Windows Authentication Proxies (WAP)s? You can replace those with a click of a button with the APM. Access Policy Manager is also great at fronting VDI and offloading authentication, for example with VMware

Horizon/View VDI you can eliminate the security servers by using APM. Similarly if you're using Citrix VDI, you can eliminate Storefront altogether. APM is heavily used in the Federal govt integrating with Common Access Cards (CAC)s. You can even use the APM to pre-authenticate ADFS traffic without the need for the traditional ADFS proxy servers. The APM also plays a hand in protecting APIs and can be used as part of F5's solution as an API Gateway.

- 500 concurrent user sessions; scalable up to 200,000
- BYOD enablement
- Full proxy for VDI (Citrix, VMware)
- Single sign-on enhancements (Identity federation with SAML 2.0)

Advanced Web Application Firewall (AWAF) – Formerly known as the Application Security Manager (ASM), true to its name the AWAF is the most advanced web application firewall on the market. While everyone was resting on their web security laurels, F5 was hard at work building the future of WAFs, extending protection past the application and on to the end-users with features like Behavioral DoS/ BaDoS extending protection to layer 7 – modeling and learning how good actors use applications to block bad actors. It's important to mention, the AWAF can also play a role in protecting APIs and has built in policies to protect them – allowing you to do schema validation and ingest OpenAPI specification files – sometimes referred to by folks as "swagger docs". OpenAPI integration with F5's WAF is useful in a CI/CD environments. Using a CI/CD pipeline, the security policy can be regularly and automatically updated.

Threat Campaigns (TC) – This is an add-on module for F5's AWAF and has come from all the good work F5's Threat Research team is doing – monitoring malicious activity around the globe and creating signatures specific to these exploits. While this is important, definitely the bigger reason to ensure you include TC with AWAF is the live updates for Bot signatures.

IP Intelligence (IPI) – it can save you a ton of bandwidth, and subsequently processing power on the downstream equipment and servers / instances. IPI is essentially a subscription for the de facto standard of bad actors database offered by Websense/Forcepoint. Since this traffic is processed at a higher level it can get dropped very early in the life of a packet and reduce a ton of strain on your environment.

- PCI-compliant web application firewall
- Anti-Bot Defense against Credential Stuffing
- L7 DDos & Behavioral DoS
- Continuous Attack Signature updates
- OWASP Compliance Dashboard
- Data Safe

	• Web scraping prevention • Integrated XML firewall • Violation correlation and incident grouping • Application DDoS protection Notă: Datasheet cu descrierea detaliată pentru fiecare modul din componența soluției ofertate sunt anexate cu oferta.