		ForcePoint
	Tip: Soluție de protecție a accesului la rețeaua Internet - Internet Gateway (proxy), inclusiv 12 luni de suport și subscriere de la producător.	
	Cerințe de licențiere:	
	Modelul de licențiere propus trebuie să acopere 400 utilizatori, inclusiv 1 instanță;	Yes
	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 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).	Yes
1.	**Caracteristici tehnice și de compatibilitate cu infrastructura BNM:**	
	Soluția trebuie să se poată instala în infrastructură în următoarele modB7:B27uri: Inline Proxy, Transparent/WCCP Proxy, Explicit Proxy, Routed Proxy;	Yes
	Suport la configurația High Availability;	Yes
	Virtual appliance de tip on-premise;	Yes
	Suport multiplatformă de virtualizare (VMware 7, Citrix XEN 8.x);	Partially, (Vmware- yes, Citrix - manually created Linux-based virtual appliance)
	Soluția trebuie să poată acționa ca proxy explicit pentru următorul tip de trafic: HTTP și HTTPS, FTP și FTPS;	Partially, the solution does not support FTPS
	Soluția trebuie să permită următoarele moduri de autentificare: NTLM, RADIUS, Active Directory, LDAP, Kerberos, Local user accounts (utilizatori stocați în baza de date a proxy-ului), Token One-Time-Password;	Yes
	Soluția trebuie să ofere un serviciu de găzduire web unde se poate găzdui scriptul de configurare proxy de tipul .pac;	Yes

Digitally signed by Abramov Ivan
Date: 2022.06.18 17:18:26 EEST
Reason: MoldSign Signature
Location: Moldova

Soluția trebuie să permită pe viitor posibilitatea de configurare în mod cluster a 2 instanțe cu disponibilitate ridicată și distribuire de sarcină automată între noduri (HA available as active-active and active-backup with session synchronization);	Yes
Soluția trebuie să fie capabilă să-și sincronizeze ceasul intern prin NTP;	Yes
Soluția trebuie să utilizeze DNS caching pentru a reduce încărcarea pe serverele de DNS;	No
Soluția trebuie să permită segregarea rolurilor pentru raportare, configurare, administrare politici și reguli;	Yes
Soluția trebuie să permită restricționarea accesului administrativ la o singură interfață de rețea;	Yes
Soluția trebuie să auditeze acțiunile administratorilor, păstrând cel puțin următoarele informații:	Yes
Timpul la care s-a produs modificarea	Yes
Cine a produs modificarea	Yes
Ce acțiune a fost luată	Yes
Pe ce obiect a fost luată acțiunea	Yes
Noua valoare a obiectului modificat;	Yes
Soluția trebuie să permită împingerea evenimentelor de audit automat pe o soluție SIEM;	Yes
Soluția trebuie să permită configurarea unei sarcini automate ce transferă backup-ul configurației pe un alt server;	Yes
Soluția trebuie să permite instalarea în mediu virtual.	Yes
Cerințe Antimalware:	
Soluția trebuie să folosească motoare de scanare antivirus;	Yes
Soluția trebuie să folosească euristice în identificarea și blocarea conținutului malițios de următoarele tipuri: Fișiere executabile, JavaScript, Flash ActionScript, Java Applets, ActiveX, Windows DDL, Scripturi Visual Basic;	Yes
Integrare cu Sandbox Cloud (inclus în subscriere);	Yes
Soluția trebuie să-și facă update pentru motoarele de scanare antivirus cel puțin o dată pe zi;	Yes
Soluția trebuie să ofere protecție și împotriva atacurilor de tip Zero-Day;	Yes

2.	Soluția trebuie să dețină un mecanism pentru protecția de scurgeri de date (DLP – Data Leak prevention) bazat pe filtre, care să permită blocarea sau jurnalizarea scurgerii informației sensibile după cuvinte cheie.	Yes
	Soluția trebuie includă protecție IPS (Intrusion Prevention System) bazat pe semnături ale vulnerabilităților și exploite-urilor cunoscute. De asemenea trebuie să includă protecție la SQL injection, domain generation algorithm attacks, java and flash exploits.	This criteria for other solution for example NGFW or WAF
	Soluția trebuie să identifice și să blocheze transmisii după comportament:	Yes
	- Furt de date: keylogger, backdoor, spyware	Yes
	- Compromitere sistem: exploatare vulnerabilități browser, execuție de cod prin exploatare vulnerabilități, software de tip troian	Yes
	- Activitate ascunsă: Rootkit, injectare de cod	Yes
	- Replicare virală: vierme de rețea, virus ce infectează fișiere	Yes
	- Amenințări web: corss site scripting, ActiveX vulnerabil	the criteria cross site scripting from WAF
	Scanarea antivirus trebuie să se facă prin captive portal și data trickling;	Partially
	Soluția trebuie să își actualizeze automat semnăturile antivirus cel puțin zilnic.	Yes
3.	**Cerințe față de filtrarea site-urilor:**	
	Soluția trebuie să permită blocarea site-urilor web după:	Yes
	Categorie de site (Ex: Social Networking, Streaming Media, etc.);	Yes
	Categorie de risc (Ex: High Risk, Medium Risk,etc.);	Yes
	Listă statică cu nume de site-uri web;	Yes
	Listă statică cu IP-uri la care sunt găzduite site-uri;	Yes
	Soluția trebuie să permită activarea acțiunii de coaching în locul blocării pentru a avertiza utilizatorii despre riscul la care se supun dacă doresc să continue la site-ul dorit;	Yes
	Soluția trebuie să permită suprascrierea locală a clasificării unui site din baza de date furnizată de producător. (Ex: Un site considerat de Social Networking să poată fi clasificat local de Business);	Yes
	Soluția trebuie să permite copierea politicilor și regulilor pentru a ușura procesul de configurare;	Yes

	Soluția trebuie să permită modificarea paginilor de notificare prezentate utilizatorilor;	Yes
	Soluția trebuie să permită blocarea site-urilor după țara în care acestea sunt găzduite;	Yes
	Soluția trebuie să verifice validitatea certificatelor SSL în cazul site-urilor securizate;	Yes
	Soluția trebuie să ofere capabilități de inspecție a traficului SSL (man in the middle).	Yes
4.	**Cerințe față de Control de aplicații:**	
	Soluția trebuie să permită blocarea de aplicații ce sunt tunelate prin proxy;	Yes
	Soluția trebuie să vină cu o bază de date de aplicații furnizată de producător și actualizată de acesta cel puțin o dată pe lună;	Yes
	Soluția trebuie să vină cu o bază de date de aplicații ce le împarte în categorii și nivel de risc.	Yes
5.	**Cerințe față de control de conținut:**	
	Soluția trebuie sa permită analiza real-time a conținutului grafic pentru a detecta conținut grafic malițios în cadrul paginilor-web (Content Analysis Service).	No
6.	**Cerințe față de raportare:**	
	Soluția trebuie să raporteze statistici despre: Trafic Instant Messaging, Trafic Web, Malware, Tipuri de fișiere, Certificatele digitale verificate, URL Filtering, Web Cache, Trafic pe internet/utilizator, Aplicații web folosite;	Yes
	Rapoartele trebuie să poată fi exportate în cel puțin următorul format: PDF;	Yes
	Rapoartele trebuie să poată fi automat transmise pe/prin e-mail;	Yes
	Soluția trebuie să ofere statistici de performanță ale sistemului: CPU, Memorie, Lățime de bandă, Cereri/secundă, etc;	Yes
	Soluția trebuie să permită investigarea logurilor de acces la internet.	Yes
7.	**Cerințe minime pentru perioada de suport și subscriere oferite de producător:**	
	12 luni din data acceptanței soluției;	Yes

	suport prin e-mail sau conectare de la distanță de la producător.	Yes
	Notă:	
	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.	Yes
	Alte cerințe obligatorii:	
	În costul ofertei trebuie să fie incluse activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe către administratorii Cumpărătorului.	Yes