R O M Â N I A
MINISTERUL PUBLIC
DIRECŢIA NAŢIONALĂ ANTICORUPŢIE
Cod fiscal 14838148

APROB,
PROCUROR ŞEF

CAIETUL DE SARCINI

Caietul de sarcini face parte integrantă din documentaţia pentru elaborarea ofertei şi constituie ansamblul cerinţelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnica şi financiară.

Cerinţele impuse prin prezentul **Caiet de sarcini** vor fi considerate ca fiind **minimale**. În acest sens oferta de bază prezentată, care se abate de la prevederile **Caietului de sarcini**, va fi luată în considerare, dar numai în măsura în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerinţelor minimale din Caietul de sarcini.

Obiectul prezentei proceduri de achiziţie publică îl reprezintă achiziția a mai multe loturi:

Lotul numărul 1 este compus din un șasiu blade, 2 module switch blade și accesorii, 4 servere blade, un rack și accesorii, un ups, un echipament de backup pe banda, 2 echipamente de stocare, instalare, configurare si servicii migrare.

Lotul numărul 2 este compus din 240 stații de lucru.

Lotul numărul 3 este compus din 65 stații de lucru mobile.

Lotul numărul 4 este compus din 15 echipamente firewall de tip A și 1 echipament firewall de tip B.

Lotul numărul 1 are specificațiile tehnice minime de mai jos :

Caracteristici șasiu blade	Solicitare
Dimensiune	Minim 10 U.
Capacitate instalabila de servere blade	Suport pentru cel puțin 16 servere blade (half-height).
Sloturi de interconectare	Suport pentru minim 8 module de interconectare redundante.
Management	2 module de management cu KVM, redundante, altele decât cele ale serverelor blade; Modulul de management trebuie să aibă acces la toate serverele blade instalate în șasiu, să poată raporta informații despre inventarul echipamentelor din șasiu, despre starea termica și a consumului de putere în timp real per server și per șasiu.
Surse de alimentare	4 surse hot plug redundante maxim 2500W fiecare.
Ventilatoare	Ventilatoare hot plug redundante.
Management șasiu și servere	Procesor de management dedicat prin care să se poată: - asigura set-up-ul și controlul întregului șasiu; - inventaria toate dispozitivele din șasiu ; - obține informații legate de temperatura și consum în timp real pentru fiecare server în parte, precum și pentru întregul șasiu; Aplicație de management dedicată, compatibilă și certificată de către producătorul de servere care asigură atât managementul serverelor fizice cât și al serverelor virtuale, intr-un mod unitar. Aceasta va asigura vizibilitatea stării de funcționare pentru întreg ansamblul pe o pagină unică, permițând investigarea diferitelor alarme prin accesarea detaliilor prin selectări simple cu mouse-ul, fără a fi necesar să lucreze în aplicații multiple; Aplicația va dispune de următoarele capabilități: - Un motor de căutare rapid ce va indexa minim următoarele obiecte: 1. adrese MAC, IP și WWN-uri; 2. rețele de tip VLAN;

	3. alerte generate de sistem; 4. denumirile serverelor (hostname); 5. volume de stocare (LUN); - Posibilitatea de asignare a alertelor generate către un utilizator definit în aplicație; - Scalabilitate la minim 256 de servere gestionate de către aplicație în configurația ofertată; - Generarea de grafice cu nivele de încărcare și utilizare ale serverelor și un istoric pe o perioada de minim 1 an; - Posibilitatea setării unui nivel de bază al firmware-ului pentru întreaga infrastructură hardware, update-ul firmware-ului fiind realizat prin rețeaua de management a serverelor cu scop în eliberarea lățimii de bandă din rețeaua de producție; - Suport pentru definirea de șabloane pentru provizionarea și configurarea serverelor; - Măsurarea condițiilor termice de operare și afișarea parametrilor prin intermediul unei interfețe 3D pentru a facilita identificarea punctelor reci/calde din interiorul unui rack/datacenter; Software-ul de management trebuie să expună prin intermediul unei interfețe de programare instrucțiuni de tipul: - Power ON/OFF; - Setări de BIOS și adrese IP; - Colectare de date și monitorizare de resurse; - Monitorizare de alerte printr-o modalitate ce nu implică interogarea continuă pentru date/stări de sistem a software-ului de management de către aplicațiile externe; - Export de date în diferite formate; Software-ul de management va suporta conexiuni de la echipamente mobile de tip smartphone bazate pe sisteme de operare Apple iOS și Android; Software-ul de management va oferi capabilități de rulare/funcționare în mediu virtual.
Altele	Șasiul să dispună montat frontal un dispozitiv de afișare pentru a ușura configurarea inițiala a șasiului și a furniza informații despre starea și operarea șasiului: consum de putere, informații despre serverele blade: procesoare, interfețele de rețea, etc. Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Caracteristici modul switch blade și accesorii	Solicitare
Descriere	modul de conectivitate cu 24 porturi.
Viteza conectivitate/port	10 Gb Ethernet.
Tip conexiuni/modul de conectivitate	16 downlinks către servere. 8 uplinks către rețea ce vor asigura o lățime de bandă de 160Gbps; Conexiune între switch-uri de 20Gbps internă sau externă, fără a folosi cele 8 porturi dedicate uplink-ului către rețea; Modulul va fi livrat cu următoarele: - 4x 10 Gb SFP+ LC SR; - Cabluri aferente 3 metri.
Management	Consola de tip web pentru provizionare și management rețele; Capabilități de tip SNMP v1, v2, v3,SSHv2; Suport pentru capabilități de tip SDN.
Securitate	TACACS+; RADIUS.
Conectivitate Cisco Catalyst 3750-X 24p (deținut de solicitant) cu switch-ul blade	Modul cu 2 porturi 10 Gb SFP+; 2 transceivere de 10 Gb SFP+ SR LC, Multimode, 850 nm; 2 cabluri aferente.
Altele	Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Caracteristici server blade	Solicitare
Dimensiune server	Mărime redusă (half-height server).
Procesor	Tip procesor – multicore; frecvență reală: 2.3 GHz; număr de nuclee: 12; cache: 25MB Level 3;
Număr de procesoare instalate	2
Număr sloturi memorie	16
Memorie RAM	Instalat: 128 GB DDR4 1600 MHz ECC Registered cu posibilitate de upgrade la 384 GB.
Protecție memorie	Advanced ECC (multi-bit error protection) sau echivalent
Procesor Grafic	Integrat care să suporte rezoluțiile: 1280 x 1024 (32bpp) 1920 x 1200 (16 bpp)
Controller RAID pentru discuri interne	Controller cu 1GB cache care să suporte RAID 0 și RAID 1 și funcționalități de accelerare și optimizare a citirii de pe discuri SSD.
Sloturi pentru extensie	2 de tip PCIe x 16
HDD-uri instalate în server	2 x 300GB 6G SAS 10K 2.5” hot plug cu suport pentru upgrade la 4 discuri de tip SSD.
Interfața de rețea	2 x 10Gb care să suporte FCoE, TCP/IP offload engine, hardware-based accelerated iSCSI, iSCSI boot.
Interfețe	1 slot intern pentru card SD; 1 port intern USB 3.0.
Management	Modul de management integrat în serverul blade cu funcții de management pentru monitorizarea stării serverului, alerte de service, și suport la distanţă ce să permită provizionarea şi configurarea serverului fără folosirea CD/ DVD.
Conform cu standardele	ACPI 2.0; USB 3.0 Support; IPMI 2.0; Secure Digital 2.0; TPM 1.2 Support; SNMP; PCIe 3.0;
Certificare pentru sisteme de operare și software de virtualizare	Serverul trebuie să fie certificat și să dispună de suport pentru cel puțin următoarele sisteme de operare: - Microsoft Windows Server 2012R2 x64; - SUSE Linux Enterprise Server (SLES) 11; - Red Hat Enterprise Linux 6; - VMware;
Sistem de operare	Windows Server 2012 R2 Standard x64.
Alte cerințe	Documentația, programele update Bios / utilitare software, driverele pentru toate componentele să fie disponibile pe pagina de web a producătorului server-ului. Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Caracteristici rack și accesorii	Solicitare
Descriere	Rack de tip enterprise compatibil cu server-ele ofertate; - Tip maxim 42U, adâncime 1200mm; - Panouri laterale detașabile; - Uși de acces în partea frontală și dorsală echipamentului; - Capacitate de încărcare minim 1300 kg; - Standarde: EIA-310D Type A, RoHS compliant; Furnizorul va asigura instalarea și punerea în funcțiune a sistemului ofertat.
KVM switch	2 x KVM switch în format rackabil cu 8porturi; 16 adaptoare pentru conexiunea la servere;
Accesorii	Kit de împământare; Kit de stabilizare și PDU;

	Se vor furniza cablurile necesare pentru interconectarea tuturor echipamentelor ofertate.
Altele	Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Caracteristici ups	Solicitare
Montare	Rack Mount.
Dimensiune	Rack maxim 3U.
Putere	5000VA / 4500 W.
Tehnologie	Line interactive.
Acumulatori	Acumulatori Hot-Swap.
Rețea	UPS Network Module.
Software de management	Da.
Altele	Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Caracteristici echipament backup pe banda	Solicitare
Dimensiune	1U.
Montare	Rack Mount.
Drive	1x drive SAS LTO6.
Slot-uri	8 sloturi de banda.
Casete	20 de casete LTO6 RW, 2 casete de curățare.
Interfata	SAS.
Interfețe management	Ethernet 10/100 , USB.
Compatibilitate	Certificat sa funcționeze cu soluția Yosemite Server Backup deținută de solicitant (listat pe pagina producătorului la categoria Device Suport).
Conectivitate cu serverul de backup existent	HBA SAS PCIe 6Gb/s compatibil cu echipamentul ofertat.
Cablu SAS	Da.
Altele	Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Caracteristici echipament de stocare	Solicitare
Echipament	Masiv de discuri cu suport pentru clusterizare.
Sisteme de management suportate de consola	Sistemul de stocare trebuie să suporte sistemele de operare din industrie, platforme și clustering, inclusiv: Windows Server 2008, Windows Server 2012,Vmware vSphere, Red Hat Enterprise, SUSE Linux, Citrix Xen Server , Oracle VM.
Capacitate	Sistemul de stocare trebuie să aibă o capacitate 24 de TB folosind discuri SAS cu 7200 rpm, de capacitate 2 TB fiecare.
Scalabilitate	Sistemul trebuie să scaleze pana la un număr de 32 de noduri Pentru optimizarea performanţei, echipamentul ofertat trebuie să ofere capabilitatea de dispersa datele sau volumele logice (LUN) pe toate discurile de același tip (tier).
Memorie	64GB RAM ; 2GB memorie cache cu baterie de protecție.
Interfețe rețea	4 interfețe 1 Gbps iSCSI pe nod, pentru conectarea la host-uri; 2 x 10Gbps porturi iSCSI pe nod.
Arhitectura și Puterea de procesare	Controler-ul este capabil să susțină funcționalitățile întregului ansamblu în caz de defectare de tip activ-activ astfel încât o singura unitate logica să poate fi accesată de ambele controlere în același timp; Extinderea numărului de noduri/controlere se va face on-line, fără a avea un impact asupra sistemul existent; Pentru a asigura o înalta disponibilitate a datelor scrise, echipamentul va suporta

	pe lângă protecția hardware de tip RAID și mai multe nivele de distribuție a datelor, într-o structură redundantă de tip cluster, între controlere pentru a preveni pierderea de date în caz de defecțiune a mai mult de un nod sau sertar de discuri; Posibilitatea de upgrade de firmware on-line, fără scoaterea sistemului din funcțiune.
No Single point of Failure	Sistemul va fi configurat pentru asigurarea unei înalte disponibilităţi cu "No Single Point of Failure" pentru controlere, memorie, ventilatoare şi surse de alimentare.
Disk Drive	Echipamentul de stocare trebuie să suporte atât tehnologii de discuri SAS, SATA de diferite dimensiuni şi viteze.
Thin Provsioning	Echipamentul de stocare să asigure fără vreo limitare de orice fel Thin Provisioning; Thin Provisioning trebuie să fie parte integrată în Sistemul de Operare și nu trebuie configurat separat ca un modul add-on.
Suport RAID	Fiecare Controller să suporte hardware-based RAID 10, 5 şi 6.
Snapshot şi replicare locală a volumelor	Echipamentul de stocare trebuie să suporte atât snapshot cât şi clone, fără alte limitări pentru întreaga capacitate suportată de echipamentul de stocare; Echipamentul de stocare trebuie să ofere suport pentru crearea de Thin Provisioning pentru provizionare snapshot şi clonă, integrare a snapshot-urilor cu aplicația; Suportă clone per volum.
Replication / Disaster Recovery	Echipamentul trebuie să suporte replicare Sincronă şi Asincronă, fără alte limitări, pentru toată capacitatea de stocare a acestuia; Să ofere suport pentru replicare sincrona de tip multi-site prin intermediul unei rețele TCP/IP cu latenţe mici; Să ofere posibilitatea replicării unui singur volum către mai multe volume; Să ofere suport de gestionare a lăţimii de bandă dedicate procesului de replicare; Să fie livrat cu o aplicație ce permite gestionarea performantelor întregului sistem.
Configurare şi Management Array	Echipamentul să fie livrat cu software pentru configurare Storage Array și software pentru Management; Software-ul trebuie să fie capabil să facă managementul la mai multe echipamente de stocare din aceeaşi familie.
Performance Management	Echipamentul trebuie livrat cu un software de măsurare a performanţelor echipamentului, fabricat de producătorul echipamentului de stocare.
Altele	Trebuie să facă parte din nomenclatorul de subansamble al firmei producătoare a sistemului.

Garanție/suport:

Echipamentele vor beneficia de garanție extinsă și suport tehnic pentru o durată de 3 ani de la data finalizării instalării acestora. Se vor asigura servicii de garanție care să garanteze reparația defecțiunilor hardware suferite în cel mult 6 ore de la plasarea solicitării de suport.

Se va asigura acces la elementele de proprietate intelectuală (drivere, firmware, actualizări software de bază) pe toată durata perioadei de garanție extinsă.
Fereastra de acoperire va fi 24x7, inclusiv zilele de sărbători legale.

Servicii de instalare:

Furnizorul va efectua și serviciile de instalare și configurare ale acestor echipamente astfel încât să obțină funcționalitatea de baza a acestora, astfel:

- Instalarea fizică a șasiului de servere lamelare și a serverelor aferente, împreună cu toate modulele de interconectare. Pornirea inițială a sistemelor și verificarea stării de funcționare.
- Instalarea fizică a sistemului de stocare a datelor în conformitate cu specificațiile tehnice ale produsului (include instalarea fizică a discurilor,cablarea echipamentului și verificarea cablării, precum și conectarea echipamentului la linia de alimentare).
- Crearea unei structuri de discuri logice pe sistemul de stocare a datelor:
  Acest serviciu include activitățile necesare pentru design-ul și implementarea structurii de discuri virtuale pe echipamentul de stocare a datelor ce va fi achiziționat ca parte a soluției.

Serviciul include și verificarea funcționalității volumelor virtuale create și prezentarea acestora către host-urile ce se vor conecta la volumele implementate.

Servicii migrare Active Directory și mesagerie electronică în mediu virtual.

Situația actuală:

Beneficiarul are implementat Microsoft Active Directory 2003 într-o arhitectura cu un forest și un singur domeniu. Site-ul este compus din 2 servere fizice cu rol de Domain Controller. Sistemul de operare instalat pe servere este Windows Server 2003 R2 SP2.
Beneficiarul are implementată o soluție de mesagerie electronică Microsoft Exchange Server 2003 SP1. Sistemul de operare instalat pe servere este Windows Server 2003 R2 SP2.
Serverele au următoarele roluri:

- 2 servere fizice cu rol de back-end;
- 1 server fizic cu rol de front-end, acces Outlook Web Access şi Exchange Server ActiveSync;

Beneficiarul dispune de licențe exchange server standard, licențe sistem de operare server standard, licențe client, precum și de resurse hardware pentru realizarea cerințelor tehnice.

Cerințe tehnice:
Upgrade-ul componentei Active Directory la versiunea 2012 R2 (un server fizic şi unul virtual).
Upgrade-ul soluției de mesagerie electronică la versiunea Exchange 2013 Standard (2 servere virtuale multirol, 1 DAG, 1 cas array).

Lotul numărul 2 cuprinde 240 staţii de lucru compuse din unitate centrală, monitor, sursă neîntreruptibilă de curent cu specificațiile tehnice minime de mai jos :

Caracteristici unitate centrală	Solicitare
Chipset placa de bază	Q85 Express sau echivalent
Placa de bază	Fabricat sub aceeași marca cu sistemul de calcul.
Procesor	Intel Core i5 3.30 GHz, cache 6MB, generația a 4-a sau echivalent
Memorie RAM	1 x 4 GB DDR3, 1600 MHz , non-ECC,
Sloturi Memorie	4 DIMM-uri
Stocare HDD	SSHD Hibrid, 1TB, SATA 6.0 Gb/s, 7200 rpm, flash 8GB
Unitate optica	DVD Writer SuperMulti, interfata SATA
Modul audio	Integrat, HD audio codec Speaker intern integrat 1.5 watt
Modul grafic	Integrat, HD Graphics 4600 sau echivalent
Interfața rețea	RJ45 Gigabit Ethernet integrat, capabil WOL, PXE, DMI, AMT 8.0 suport
Sloturi I/O	3 x PCI-Express x1 low profile 1 x PCI-Express x16 low profile
Porturi I/O spate	4 x USB 2.0, 2 x USB 3.0, 2 x DisplayPort (su suport multi-stream), 2 x PS/2, 1 x VGA, 1 x RJ45, 1 x Audio intrare, 1 x Audio ieșire, 1 x port serial
Porturi I/O faţa	2 x USB 2.0, 2 x USB 3.0,1 x Microfon, 1 x Căști
Lăcașe fixe pentru unități HDD sau DVD	1 x 3.5 inch intern 1 x 2.5 inch intern 1 x 3.5 inch extern
Tastatură	PS/2, cu caractere romanești. Fabricată sub aceeași marca cu sistemul de calcul.
Mouse	USB, optic, 2 butoane, scroll. Fabricat sub aceeași marca cu sistemul de calcul.
Sursa de alimentare	Intrare 220V/50Hz, Putere minimă 240W, eficienţă 90% . PFC Activ.
Carcasă	Tip: Small Form Factor (SFF) Carcasă cu acces ușor de tip „tool-less” și cu posibilitatea unei schimbări ușoare a componentelor.
Culoare carcasa	Neagră.
Dimensiuni carcasa (Lățime x Înălțime X Adâncime)	Maxim : 100 mm x 400 mm x 350 mm

Securitate	Modul de securitate (tip TPM) integrat pe placa de bază. Posibilitatea de a bloca/debloca porturile USB și Serial din BIOS Posibilitate dezactivare SATA din BIOS Posibilitate de a seta parole pentru BIOS și pornirea sistemului Carcasa trebuie să fie dotată cu un dispozitiv mecanic cu senzor care să detecteze deschiderea neautorizată a carcasei.
Sistem de operare	FreeDOS sau fără sistem de operare.
Standarde și Certificări	- Siguranța în exploatare: IEC60950 - - Compatibilitate electromagnetica: EN55022, EN55024 - Epeat Gold - Energy Star - ISO 9001, ISO 14001; sau echivalente.
Conformitate cu sisteme de operare	Sistemul de calcul de tip Desktop trebuie să fie listat de Microsoft în Windows 7 sau Windows 8 Hardware Compatibility List (HCL), sectiunea Sistems/Desktop PCs. Monitorul trebuie să fie listat de Microsoft în Windows 7 sau Windows 8 Hardware Compatibility List (HCL), secțiunea Monitors&Displays/LDC Monitors.
Garanție Producător	3 ani de tip next business day on-site pentru întreg sistemul
Accesorii	1 x pereche boxe audio de putere 2W, cu jack de 3.5 mm pentru ieșire căști și control volum. 1 x mouse pad. 1 x cablu de rețea de 5 m. Cablu de alimentare. Documentație în format electronic pe mediu optic. Orice alt accesoriu necesar instalării și punerii în funcțiune.
Nota	Nu sunt acceptate adaptoare sau soluții improvizate pentru porturile si interfețele echipamentului

Caracteristici monitor	Solicitare
Monitor	Fabricat sub aceeași marca cu sistemul de calcul.
Diagonala	20 inch
Format	16:9
Tehnologie	LED Backlit, antiglare
Rezoluție	1600 * 900 @ 60 Hz
Unghiuri de vizualizare	160 orizontal / 160 vertical
Luminozitate	250 nits
Inclinare	-5 grade -> 30 grade
Rotire	360 grade
Ajustare înălțime	150 mm
Timp tipic de răspuns	5 ms
Video input	VGA , DVI-D, DisplayPort
Consum	Maxim 30W
Certificări	TCO 06, EPEAT GOLD, ENERGY STAR sau echivalente
Accesorii	Cablu de alimentare, Cablu VGA analog și DisplayPort

Caracteristici Sursă neîntreruptibilă de curent	Solicitare
Alimentare	220-240 V / 50 Hz
Putere	400 VA
Indicator vizual	Da
Indicator acustic	Da
Conectori intrare	1 de tip Schuko CEE 7/7 Plug
Conectori ieșire	6 de tip Schuko CEE 7 Plug , minim 4 pe baterie

Baterie	Sigilată cu protecție la scurgeri de lichid.
Timp mediu de funcționare	15 minute la 50% încărcare
Protecție	La supraîncărcare, suprasarcină, descărcări electrice
Management	Nu
Greutate	Maxim 6 Kg

Garanția pentru toate echipamentele din Lotul numărul 2 să fie de 3 ani , acordată la sediul clientului cu un timp de răspuns de maxim o zi lucrătoare de la sesizarea defecțiunii.

Lotul numărul 3 este compus din 65 stații de lucru mobile cu specificațiile tehnice minime de mai jos :

Caracteristici stație de lucru mobilă	Solicitare
Tip procesor:	Intel Core i5-4210M 2.6 GHz, cache 3MB, generația a 4-a sau echivalent
Chipset:	Mobile Intel HM87 Express sau echivalent
Diagonală:	15.6 inch
Rezoluție	1920 x 1080
Tehnologie display	TFT LED-backlit FHD, antiglare
Camera Web	Da
Memorie Instalată	8GB DDR3
Memorie Maximă	Expandabilă la 16GB
Capacitate Hard Disk	500 GB, 7200 rpm SATA
Placa video	Integrată, Intel HD Graphics 4600 sau echivalent
Unitate optică internă	DVD-RW
Audio	HD DTS Sound, Boxe stereo integrate Microfon intrare Audio/căști intrare
Comunicații	Placa de rețea integrata Gigabit (10/100/1000 Mbps) Wireless 802.11 b/g/n WLAN cu 2 antene Bluetooth 4.0
Pointing Device	Touchpad
Porturi I/O	1 x DisplayPort 1.2 1 x RJ-45 4 x USB 3.0, din care unul cu încărcare 1 x VGA 1 x serial 1 x căști, 1 x microfon 1 x DC-in 1 x Docking conector 1 x Cititor carduri de memorie – SD,SDHC,SDXC
Carcasa	Rezistenta la șocuri
Tastatura	Standard, cu bloc numeric
Cablu de alimentare:	Da
Alimentator extern	Suport pentru standardele românești: 220V / 50 Hz
Baterie	6 celule Li-Ion
Autonomie de lucru	10 ore
Securitate	Modul de securitate tip TPM/TCPA integrat. Sistem de protecție a datelor de pe HDD atât software cat și hardware (cu posibilitatea parcării automate a capetelor HDD-ului la bruscarea sistemului)

	Cititor/scanner de amprenta digitala integrat în carcasa. Soluție dedicată (diferită de simpla ștergere a datelor sau formatarea HDD-ului) capabilă să șteargă informaţiile critice de pe HDD
Greutate	Maxim 2,5 Kg cu bateria inclusa
Geantă transport:	Da
Sistem de operare:	Windows 8.1 Pro 64bit
Standarde și Certificări	- EN 60950, IEC 950, FCC - ISO 9001, ISO 14001;
Drivere	Livrate pe suport optic pentru Windows 8.1 sau pe pagina web a producătorului
Garanție producător	3 ani (garanția producătorului) inclusiv pentru baterie

Lotul numărul 4 este compus din :

15 echipamente firewall de tip A ce au specificațiile tehnice hardware minime în tabelul 4.3 și functionalitățiile modulelor software în tabelul 4.1

1 echipament firewall de tip B ce are specificațiile tehnice hardware minime în tabelul 4.2 și functionalitățiile modulelor software în tabelul 4.1

Cerințe generale :

Echipamentele ofertate trebuie să fie capabile să acopere toate cerințele legate de performanta, lățime de bandă, număr total de conexiuni și număr de conexiuni pe secundă, cât și funcții avansate de securitate de tip next generation security gateway (vezi tabelul 4.1 de mai jos).

Echipamentele firewall trebuie să se integreze nativ în soluţia firewall de management, raportare şi monitorizare Check Point, existentă la beneficiar şi să prezinte caracteristicile tehnice minime obligatorii de mai jos. Soluţia firewall Check Point existentă la beneficiar este o soluţie cu management centralizat ce rulează versiunea R75.47 (sau R77.20).

Funcționalitățile de tip next generation security gateway, ca de exemplu IPS, controlul aplicațiilor, filtrare URL, anti-virus.. să poată fi administrate cu ajutorul unei platforme de management unică și centralizată.

Servicii de instalare și configurare:

Ofertantul va oferi servicii de instalare și configurare pentru echipamentele ofertate. Toate serviciile se vor presta la sediul beneficiarului din București.

Next generation security gateway trebuie să suporte, pe o platforma unificată, următoarele funcţionalităţi:

1. Firewall de tip Stateful Inspection
2. Sistem de detecție și prevenție a intruziunilor (IPS)
3. Achiziţia și identificarea utilizatorilor
4. Controlul aplicațiilor Internet și filtrare URL
5. Anti-virus
6. Anti-Spam și securitate e-mail
7. IPSecVPN
8. Accesul dispozitivelor mobile (Windows, Android, IOS) folosind SSLVPN
9. Sistem de management al politicilor de securitate
10. Sistem de analiza a log-urilor

Topologie:

Soluția de securitate oferita trebuie să asigure protecția unui nou birou din București şi cincisprezece (15) sedii din teritoriu.

Conectivitatea între sediul central şi celelalte sedii trebuie să fie de tip stea IPsec VPN, managementul întregii soluții de securitate şi al tunelelor VPN trebuie să fie făcut din sediul central.

Tabel 4.1 :

Caracteristici module software	Solicitare
Punctul 1 : Functionalitati Firewall de tip Stateful Inspection	să utilizeze mecanisme de filtrare a conexiunilor bazate pe informațiile legate de starea acestora; să suporte toate specificațiile legate de performanţa cerută, lățime de bandă, număr total de conexiuni și număr de conexiuni pe secundă; să suporte și să controleze accesul la cel puțin 150 de servicii și protocoale de comunicație predefinite; în cadrul soluției de management aferenta modulului, trebuie să existe suport pentru contorizarea accesului la fiecare regulă de securitate definită, folosind un „hit counter” unic și specific fiecărei reguli de firewall; Să permită definirea obiectelor de tip timer pentru a permite sau restricționa accesul la anumite reguli de securitate, în funcție de ora și data sistemului, și să ofere capabilități de expirare predefinita a regulilor de securitate; Comunicația dintre firewall și serverul de management să fie criptata și bazata pe certificate de tip PKI emise de către o autoritate de certificare locală și integrată în soluția de securitate; Să suporte metode de autentificare a utilizatorilor de tip user,client și sesiune; Să suporte următoarele scheme de autentificare: TACACS, RADIUS, tokens(SecureID) și certificate digitale emise local, în cadrul soluției sau de către autorități publice; Să conțină o baza de date locala a utilizatorilor, pentru a permite autentificarea și autorizarea acestora, astfel încât să nu fie necesara o soluție externa de management; Să aibă suport pentru alocare dinamica de adrese IP folosind protocolul DHCP server și relay; Să suporte proxy HTTP și HTTPS; Să fie capabila să lucreze în mod transparent (bridge mode); Să ofere suport pentru gateway high availability (cluster HA) și distribuție load sharing (cluster LS).
Punctul 2 : Funcționalități Sistem de detecție și prevenție a intruziunilor IPS	Să folosească mecanisme de detecție a atacurilor bazate pe : semnături, anomalii de protocol, controlul aplicațiilor și comportamentul acestora; Modulul de IPS și cel de Stateful Inspection trebuie să fie integrate pe aceeaşi platformă; Să ofere opțiunea de a defini profile IPS pentru client sau server, sau o combinație de amândouă; Să ofere ce puțin două profile/politici IPS predefinite; Să folosească un mecanism software de tip fail-open, configurabil în funcție de încărcarea procesorului (CPU) și a memorie (RAM); Să ofere un mecanism automat pentru activarea și administrarea noilor semnături prevenite din update-uri; Să suporte adăugarea de excepții bazate pe sursa și destinația traficului sau serviciului, indiferent de combinația acestora; Să includă o metodă de investigare a problemelor, care să poată să fie activată la nivelul fiecărui profil (IPS) prin intermediul unui

	singur buton, aceasta trecând protecțiile din modul prevenție în modul detecție; Să ofere un mecanism centralizat de corelare și raportare a evenimentelor; Administratorul să poată activa noile protecții provenite din update-uri, bazat pe parametrii configurabili (impactul asupra performanţei, severitatea amenințărilor, nivelul de încredere, protecția clientului, protecția serverului); Să poată detecta și preveni următoarele amenințări: folosirea necorespunzătoare a protocoalelor, comunicația folosită în scopuri distructive, atacuri asupra tunelelor VPN și atacurile generice care nu au semnături; Sa includă pentru fiecare protecție, tipul acesteia (orientată către server sau către client) gradul amenințării, nivelul de încredere și referințe; Să poată captura pachete de date pentru toate protecțiile active; Să detecteze și blocheze atacurile la nivel rețea și aplicații, protejând cel puțin următoarele servicii: e-mail, DNS, FTP, SNMP, servicii Windows; Să includă posibilitatea de a detecta sau bloca traficul peer to peer, folosind tehnici evazioniste; Administratorul să poată defini excluziuni de rețea și de host de la inspecția IPS-ului; Să ofere protecție împotriva DNS Cache Poisoning; Să ofere protecție pentru protocoalele VOIP; Să detecteze și să blocheze aplicațiile de tip control remote, inclusiv cele capabile să tuneleze traficul specific prin intermediul protocolului HTTP; Să ofere protecții SCADA; Să aibă un mecanism de conversie a semnăturilor SNORT în semnături specifice; Să poată bloca traficul inbound și/sau outbound în funcție de zone geografice, ţări, fără să fie nevoie de se definească grupuri de IP-uri corespunzătoare zonelor geografice vizate.
Punctul 3 : Funcționalităţi Achiziția și identificarea utilizatorilor	Să verifice identitatea utilizatorului, folosind Microsoft Active Directory, pe baza evenimentelor de securitate; Să aibă o metoda de autentificare bazata pe browser Web pentru achiziția identităţii unui utilizator sau a obiectelor din afara domeniului AD; Să aibă un client dedicat, instalabil prin politica de securitate pe computerele utilizatorilor, și care să poată dobândi și raporta identităţi către soluția de securitate; Să suporte funcționarea pe infrastructura servere de terminale; Impactul asupra controlerelor de domeniu să fie mai mic de 4%; Să dobândească identitatea utilizatorilor de la Microsoft Active Directory, fără să instaleze un agent pe controlerele de domeniu; Să suporte autentificare transparenta Kerberos pentru Single Sign On; Să suporte utilizarea de grupuri LDAP imbricate; Să poată partaja sau propaga identităţi de utilizatori între mai multe gateway-uri de securitate; Să poată crea roluri de identitate utilizabile în toate modulele software din cadrul soluției de securitate.
Punctul 4 : Funcționalităţi filtrare trafic web și	Baza de date de control de aplicație trebuie să conțină 6000 de aplicații cunoscute;

controlul aplicațiilor internet	Să ofere un control de securitate granular pentru 260000 de wiget-uri Web 2.0; Să aibă o clasificare URL care să cuprindă cel mult 200 milioane de URL –uri și acoperă mai mult de 85% din top 1.000.000 de site-uri Web; Să poată să creeze reguli de filtrare conținând mai multe categorii; Să poată să creeze reguli de filtrare pentru un site care să fie în categorii multiple; Să permită granularitate în definirea politicilor de securitate la nivel de utilizatori și grupuri de utilizatori; Memoria cache locală de pe gateway-ul de securitate trebuie să dea răspunsuri în proporție de 99% la cererile de categorisire URL-uri, în termen de 4 săptămâni de la punerea în producție; Să aibă o interfața ușor de utilizat, pentru căutare de aplicații și URL-uri; Să clasifice aplicații și URL-uri în funcție de factorul de risc; Să poată defini pe baza identității utilizatorilor, controlul aplicațiilor și politica de securitate URLF; Să actualizeze printr-un serviciu în cloud a controlului aplicațiilor și baza de date URLF; Să aibă reguli unificate pentru controlul aplicațiilor și normele de securitate URLF; Să furnizeze un mecanism de informare a utilizatorilor, în timp real, cu scopul de a-i educa cu privire la politicile de securitate implementate; Să permită excepții bazate pe obiecte definite de rețea; Să ofere posibilitatea de a modifica mesajul de notificare în caz de blocare a utilizatorului, atunci când acesta încearcă să acceseze o aplicație Internet, și de a redirecționa utilizatorul la o pagina de remediere a incidentului de securitate; Să includă un mecanism de management a listelor negre și albe, pentru a permite administratorului să refuze sau să permită URL-uri specifice, indiferent de categorie; Să ofere un mecanism de corecție în ceea ce privește clasificarea URL-urilor; Să raporteze cu privire la numărul de accesări al fiecărei reguli configurate.
Punctul 5 : Funcționalități antivirus	Să aibă o componentă Anti-Virus integrată pe firewall-ul de generație următoare; Politicile Anti-Virus trebuie să fie administrate intr-o consolă centrală; Să folosească un mecanism centralizat de corelare și raportare a evenimentelor de securitate; Să fie în măsura să prevină accesul la site-uri infectate sau suspectate drept malițioase; Să fie capabil de a inspecta trafic criptat SSL; Să fie actualizat în timp real de la un serviciu locat în cloud; Să fie capabil să oprească fișiere malware conținute în traficul de intrare în rețeaua locală; Politicile să fie gestionate centralizat cu posibilitate de configurare și aplicare selectivă.
Punctul 6 : Funcționalități Anti-Spam și securitate e-mail	Să nu țină cont de limba de redactare a mesajelor; Să aibă clasificare în timp real și protecție pe baza de focare de spam detectate , care se bazează pe modele recurente și nu pe conținut;

	Să poată bloca IP-uri folosind un serviciu on-line, pentru a evita alarmele false; Să includă un mecanism de protecţie de tip “ora zero”, pentru noi viruși care se răspândesc prin e-mail și spam , fără să se bazeze exclusiv pe inspecție euristică sau de conținut.
Punctul 7 : Funcționalități IPsec VPN	Să suporte autorităţi de certificare internă (proprietară) și externe (publice); Să suporte criptare 3DES și AES-256 pentru IKE faza I și II, IKEv2 plus "Suite-B-GCM-128" și "Suite-B-GCM-256" pentru faza II; Să suporte cel puțin următoarele grupuri Diffie-Hellman: Grup 1 (768 bit) , Grup 2 (1024 bit) , Grup 5 (1536 bit) , Grup 14 (2048 bit) , Grup 19 și Grup 20; Să suporte integritatea datelor cu MD5 , SHA1, SHA-256 , SHA-384 și AES – XCBC; Să includă suport pentru VPN punct la punct în următoarele topologii : - Full Mesh (toate pentru toți) , - Stea (birourile de la distanţă la site-ul central) - Hub și Spoke (site-ul de la distanţă prin intermediul site-ul central către un alt site de la distanţă); Să suporte configurarea VPN prin intermediul unei interfețe grafice (GUI) folosind metode de tip drag and drop a obiectelor; Să suporte SSL VPN fără client pentru acces de la distanţă ; Să suporte VPN L2TP, inclusiv suport pentru client iPhone L2TP; Să permită administratorului să aplice normele de securitate pentru a controla traficul în interiorul VPN-ului; Să suporte “domain based” și “route based” VPN folosind interfața tunel virtuală (VTI) și protocoale de rutare dinamice; Să includă posibilitatea de a stabili tunele VPN cu gateway-uri cu IP-uri dinamice publice; Să includă compresie IP pentru VPN “client-to-site” și “site-to-site”
Punctul 8 : Funcționalități accesul dispozitivelor mobile (Windows, Android, IOS) folosind SSLVPN	Să aibă o opțiune de a oferi o soluție de mobilitate sigură pe deplin integrată cu firewall-ul de generație următoare; Să suporte atât dispozitive gestionate cât și dispozitive de tip BYOD.
Punctul 9 : Funcționalități Sistem de management al politicilor de securitate	Să fie capabilă să coexiste pe gateway-ul de securitate dar și independent de acesta; Să accepte împărțirea atribuțiilor administratorilor în funcție de rolul acestora. De exemplu, rol pentru managementul politicii firewall sau numai rol pentru vizualizare log-urilor; Să includă un canal sigur criptat de comunicare, bazat pe certificat între toate componentele distribuite de furnizor și care aparțin unui singur domeniu de gestionare; Să includă o Autoritate de Certificare internă X.509, care poate genera certificate de gateway-uri și utilizatori și care permite autentificarea pe VPN; Să includă posibilitatea de a folosi autorităţi de certificare externe care acceptă PKCS # 12, standardele CAPI sau Entrust; Toate aplicațiile de securitate trebuie să fie gestionate de la consola centrală; Să permită monitorizarea accesului la regulile de securitate, pe măsura ce acestea au fost aplicate pentru traficul specific, pe baza unui contoar (hit counter); Să includă o opțiune de căutare pentru a putea interoga cu ușurință care obiect din rețea conține o adresa IP specifică sau doar o parte

	din ea; Să includă opțiunea de a segmenta baza de reguli cu ajutorul etichetelor sau a titlurilor de secțiune, cu scopul de a organiza mai bine politica de securitate; Să ofere opțiunea de a salva întreaga politică sau o parte specifică a politicii; Să aibă un mecanism de verificare prealabilă a politicii de securitate înainte de instalarea politicii; Să aibă un mecanism de control de revizuire a politicii de securitate; Să aibă opțiunea de a adăuga un server de management aflat în standby, care se sincronizează automat cu cel activ, fără a fi nevoie de un dispozitiv de stocare extern; Să includă capacitatea de a distribui și de a aplica centralizat noi versiuni de software de gateway; Să includă un instrument gestiune centralizată a licențelelor de gateway-uri controlate de către stația de management; Interfaţa Grafica de Management (GUI) să poată să excludă cu ușurință adresa IP de la definiția semnăturii IPS; Prin intermediul GUI trebuie să existe posibilitatea de a ajunge cu ușurință la semnătura IPS pornind de la intrările de tip log IPS; Log Viewer-ul să poată afișa toate log-urile de securitate (FW, IPS, URLF, s.a), într-un un singur panou, pentru a simplifica procesul de depanare a problemelor de conectivitate pentru o adresă IP Log Viewer-ul să poată crea filtre folosind obiectele predefinite (clienți, rețele, grupuri, utilizatori, s.a); Log Viewer-ul să poată crea multiple "filtre salvate" personalizate, pentru utilizare la o dată ulterioară.
Punctul 10 : Funcționalități Sistem de analiză a log-urilor	Jurnalizarea centralizata trebuie să fie parte a sistemului de management. Alternativ, administratorii să poată instala servere dedicate de Log; Să ofere opțiunea de a rula pe serverul de management sau pe un server dedicat; Să fie capabilă să ruleze pe un server de tip X86 listat pe o lista de compatibilitate hardware a producătorului; Să aibă capabilitatea de a înregistra toate regulile (+30k logs/sec); Log viewer-ul să poată căuta indexat; Să poată înregistra toate aplicațiile de securitate integrate, inclusiv Firewall, IPS, Controlul Aplicațiilor și filtrare URL, Anti-Virus, Anti-Spam, Achiziție și Identitate utilizatori, DLP și controlul dispozitivelor mobile; Să includă un mecanism automat de captare de pachete pentru evenimente IPS pentru a facilita colectarea de probe ce pot fi folosite în analize de tip forensic; Să ofere log-uri diferite referitor la activitatea utilizatorilor obișnuiți și log-uri referitoare la activitatea de management; Să poată să se deplaseze de la jurnalul de log-uri de securitate la regula de securitate, cu un singur click de mouse; Pentru fiecare regulă de securitate sau tip de eveniment, soluția să ofere cel puțin următoarele opțiuni: Jurnalizare, alertă, SNMP trap, email și execuția un script definit de utilizator; Jurnalele să aibă un canal securizat de transfer de pe gateway pe log server pentru a preveni interceptarea, soluția să conțină autentificare și criptare; Jurnalele să fie transferate în siguranță între gateway și serverul de

	management sau serverul dedicat de log și consola de vizualizare a jurnalelor în PC-ul administratorului; Să includă opțiunea de a bloca în mod dinamic o conexiune activa prin intermediul log GUI fără a fi necesara modificarea regulilor predefinite; Să permită exportul de log-uri în format de baze de date; Să permită comutarea automata a fișierului care acumulează log-uri, bazat pe o oră programată sau dimensiunea fișierului; Să suporte adăugarea de excepții în IPS direct din înregistrările jurnal (log-uri); Să fie capabilă să se asocieze un nume de utilizator și nume de mașină la fiecare înregistrare jurnal; Să includă o interfață grafică de monitorizare (GUI) care să ofere o modalitate ușoară de a monitoriza starea gateway-ului; Să furnizeze următoarele informații de sistem pentru fiecare gateway: sistem de operare, utilizarea procesorului, utilizarea memoriei, toate partițiile pe disc și % de spațiu liber pe hard disk; Să ofere statusul de fiecare componenta a gateway-ului (de exemplu, firewall, VPN, cluster, antivirus, etc); Să includă starea tuturor tunelurilor VPN, site-to-site și client-to-site; Să poată seta un prag personalizabil și să ia măsuri atunci când este atins un anumit prag pe un gateway. Acțiunile trebuie să includă: Log, alert, trimite un SNMP trap, trimite un e-mail și execută o alertă definită de utilizator; Să includă opțiunea de a înregistra vizualizările de trafic și de sistem intr-un fișier pentru vizualizare ulterioară în orice moment; Să recunoască disfuncționalități și probleme de conectivitate, între două puncte conectate printr-un VPN, să log-eze și de alerteze în cazul în care tunelul VPN nu funcționează.

Tabel 4.2:

Caracteristici echipamente firewall de tip B	Solicitare
Firewall Troughput	Maxim 3 Gbps
Firewall Troughput în producție	1.3 Gbps
VPN Troughput	0.4 Gbps
IPS Troughput recomandat	0.3 Gbps
IPS Troughput în producție	0.15 Gbps
Sesiuni concurente	1.2 M
Conexiuni pe secunda	25000
VLAN's	1024
Firewall-uri Virtuale	3
Memorie RAM	2 GB
Port Consola	Da
WiFi	Nu
USB	2
PCI Express Slot	Inclus
Hard Disk	250 GB
Suport Modem 3G și 4G	Da
Kit montare rack	Da
Conectivitate Ethernet 10/100/1000	6
Suport pentru protocoale de rutare dinamice	RIP RFC 1058 RIP v2 (cu autentificare) RFC 1723 RIPng (IPv6) RFC 20801

	OSPFv2 RFC 2328 OSPF NSSA RFC 3101 OSPFv3 (IPv6) RFC 2740 BGP4 RFCs 1771, 1963, 1966, 1997, 2918 BGP4++ RFC 2545, 2858 (unicast IPv6)
Lățime	21 cm
Înălțime	4.2 cm
Adâncime	20.95 cm
Greutate	2 kg
Operating Environment	0ºC ~ 40ºC (5~95%, non-condensing)
AC Input	100 - 240 VAC
Frequency	50 - 60 Hz
Power Supply Rating	12V/2A DC 24W
Maximum Power Consumption	35 W
Maximum Thermal Output	119.4 BTU
Module software pentru echipamente firewall tip B	Solicitare
Tabelul 4.1 Punctul 1	Da
Tabelul 4.1 Punctul 2	Da
Tabelul 4.1 Punctul 3	Da
Tabelul 4.1 Punctul 4	Da
Tabelul 4.1 Punctul 5	Da
Tabelul 4.1 Punctul 6	Da
Tabelul 4.1 Punctul 7	Da
Tabelul 4.1 Punctul 8	Da
Tabelul 4.1 Punctul 9	Da
Tabelul 4.1 Punctul 10	Da

Tabel 4.3:

Caracteristici echipamente firewall de tip A	Solicitare
Firewall Troughput	Maxim 1.5 Gbps
Firewall Troughput în producție	0.3 Gbps
VPN Troughput	220 Mbps
IPS Troughput recomandat	100 Mbps
IPS Troughput în producție	30 Mbps
Antivirus Troughput	100 Mbps
Sesiuni concurente	200000
Conexiuni pe secunda	5000
VLAN’s	1024
Firewall-uri Virtuale	3
1 GbE LAN Ports	8
1 GbE WAN Port	1
1 GbE DMZ Port	1
ADSL	Nu
WiFi	Nu
USB	2
PCI Express Slot	Inclus
SD Card Slot	1
Suport Modem 3G și 4G	Da
Latime	22 cm
Inaltime	4.4 cm
Adancime	15.24 cm
Greutate	1.2 kg
Operating Environment	0ºC ~ 40ºC (5~95%, non-condensing)

AC Input	100 - 240 VAC
Frequency	50 - 60 Hz
Power Supply Rating	12V/2A DC 24W
Maximum Power Consumption	16.68 W
Maximum Thermal Output	56.9 BTU
Suport pentru protocoale de rutare dinamice	RIP RFC 1058 RIP v2 (cu autentificare) RFC 1723 RIPng (IPv6) RFC 20801 OSPFv2 RFC 2328 OSPF NSSA RFC 3101 OSPFv3 (IPv6) RFC 2740 BGP4 RFCs 1771, 1963, 1966, 1997, 2918 BGP4++ RFC 2545, 2858 (unicast IPv6)
Module software pentru echipamente firewall tip A	Solicitare
Tabelul 4.1 Punctul 1	Da
Tabelul 4.1 Punctul 2	Da
Tabelul 4.1 Punctul 3	Da
Tabelul 4.1 Punctul 4	Da
Tabelul 4.1 Punctul 5	Da
Tabelul 4.1 Punctul 6	Da
Tabelul 4.1 Punctul 7	Da
Tabelul 4.1 Punctul 8	Da
Tabelul 4.1 Punctul 9	Nu
Tabelul 4.1 Punctul 10	Nu

Garanția pentru toate echipamentele din Lotul numărul 4 să fie de 1 an , acordată la sediul clientului cu un timp de răspuns de maxim o zi lucrătoare de la sesizarea defecțiunii.

Nerespectarea cerințelor tehnice şi funcționale minimale obligatorii sau a altor cerințe obligatorii atrage automat declararea ofertei ca neconformă.

Termen de livrare pentru echipamentele hardware 30 zile.
Termen finalizare servicii de instalare, configurare si migrare maxim 60 zile după livrarea echipamentelor.

Întocmit
Specialist IT
Ciobanu Victor

Vizat
Sef Birou IT
Sterea Corneliu