SECŢIUNEA III

CAIET DE SARCINI

Cerinte Generale: Caietul de sarcini face parte integranta din documentatia de atribuire si constituie ansamblu cerintelor pe baza carora se elaboreaza de fiecare ofertant propunerea tehnica . Toate afirmatiile de conformitate vor face trimitere la capitol subcapitol, pagina din documentatia tehnica a ofertantului depusa in procedura (Manuale de instalare, configurare, exploatare)

Descriere **Soluție integrată pentru protecția informației, înregistrarea și arhivarea traficului de date**

SN Radiocomunicații SA dorește achiziționarea unei soluții unitare pentru protejarea rețelei interne de date împotriva intruziunilor, transmiterii de informații confidențiale atât prin intermediului poștei electronice cât și prin alte metode, precum și pentru arhivarea traficului de date într-o locație secundară.

Soluția va trebui să utilizeze o platformă flexibilă și sigură pentru a monitoriza și proteja informațiile, documentele electronice și alte date de natură confidențială din cadrul instituței, în mod independent de modul în care aceste date sunt folosite și indiferent de mediul de stocare pe care acestea se află. Soluția acoperă toate datele confidențiale pe stații de lucru, în rețea sau în sistemele externe de stocare. Pentru a oferi protecție completă împotriva pierderii informațiilor confidențiale, platforma permite inventarierea datelor, protecția lor – cu evidențierea încălcării politicilor de securitate, precum și crearea / aplicarea unui set unificat de politici de securitate a datelor la nivel de organizație dar și remedierea și raportarea incidentelor.

Soluția va furniza de asemenea și serviciile de acces Internet, politici de rutare și firewall pentru rețeaua WAN a SN Radiocomunicații SA.

Întreaga arhitectură este compusă din următoarele componente:

1. **Componente hardware**:

a. *echipament appliance tip UTM pentru îndeplinirea următoarelor funcționalități (2 bucăți)*:
- ✓ firewall
- ✓ IPSEC VPN
- ✓ Protecție împotriva intruziunilor (IPS/IDS)
- ✓ filtrare conținut web pe baza unor liste create și a unor baze de date centralizate ale producătorului
- ✓ protecție împotriva transmiterii de informații confidențiale în afara rețelei SNR
- ✓ înregistrare și monitorizare trafic HTTP, HTTPS, Messenger, SMTP, IMAP, POP3, VoIP

b. *echipament appliance tip EMAIL Firewall pentru îndeplinirea următoarelor funcționalități (2 bucăți)*:
- ✓ e-mail firewall
- ✓ antispam
- ✓ antivirus SMTP/POP3/IMAP
- ✓ filtrare conținut atașamente
- ✓ protecție împotriva transmiterii de informații confidențiale via e-mail
- ✓ înregistrarea tuturor e-mailurilor transmise către și dinspre SNR

c. *echipament de logging appliance care să permită întregii soluții transmiterea de loguri și generarea de rapoarte (1 bucată)*

d. *stație de calcul mobilă pentru managementul soluției (1 buc)*

2. **Componente software**:

a. *solutie software de replicare asincrona a informatiilor, atasamentelor si istoricului de trafic pentru salvarea intr-o locatie secundara*

Mod de implementare:
a. *Sediul Central*, la Sediul Central se vor regasi urmatoarele echipamente si software:

- ✓ un appliance tip UTM
- ✓ doua appliance-uri tip EMAIL Firewall
- ✓ un appliance pentru logging
- ✓ solutie software replicare HA
- ✓ agent software replicare DR

Appliance-ul UTM va securiza reteaua, fiind instalat astfel incat tot traficul generat spre spre / dinspre reteaua interna a SN Radiocomunicatii SA sa fie redirectat spre el. Acest echipament va indeplini toate functiile necesare de filtrare, va transmite loguri catre appliance-ul pentru logging.

Traficul care se doreste a fi analizat este: HTTP, HTTPS, SMTP, IMAP, POP3, VoIP, Messenger si IP. Totodata acest appliance va fi unul din capetele tunelului de VPN creat cu locatia de backup

Appliance-urile EMAIL Firewall vor proteja, analiza si inregistra traficul catre si dinspre serverele de mail SNR. EMAIL Firewalls vor transfera toate mail-urile care vor face obiectul carantinei, din diverse motive, catre appliance-ul de logging pentru arhivare.

Appliance-ul pentru logging va pastra logurile generate de toate appliance-urile din organizatie si le va transfera catre solutia interna de SYSLOG instalata pe un system Windows Server 2008 R2 in mediu virtual Hyper-V. Acest echipament va genera automat rapoarte despre trafic, informatii transmise, e-mail-uri carantinate, etc.

Pe server-ul pe care se vor stoca toate logurile, atasamentele, istoricele de trafic se va instala o solutie care sa permita urmatoarele functionalitati:

- ✓ protectie tip HA activ-pasiv cu un al doilea server instalat in aceiasi locatie
- ✓ protectie tip Disaster Recovery cu un al treilea server instalat in locatia de backup - se va adauga un agent / mediu in care se va face protectia este VMWare vSphere

Aceasta solutie trebuie sa foloseasca o consola centralizata pentru ambelele medii de protectie (HA si DR)

b. *Locatie Backup,* in locatia pentru backup se vor regasi urmatoarele componente:

- ✓ un appliance tip UTM
- ✓ solutie software DR (server imagini)

Echipamentul de tip UTM va avea rol de capat pentru tunelul VPN care va securiza transferul dintre Sediul Central si Locatia de Backup.

Solutia software pentru DR va pastra imagini generate de server-ul de logging si va permite exitenderea si catre alte servere. Totodata aceasta solutie trebuie sa permita recuperarea datelor catre un mediu fizic sau virtual.

Caracteristicele care sunt necesare pentru fiecare tip de echipament sunt enumerate in continuare:

1. *Echipament appliance tip UTM*

Denumire	**Echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată**
Configuraţie	• 20 interfețe 10/100/1000 Ethernet • 2 porturi USB • 1 port consolă

Caracteristici	• Trafic firewall calculat pentru pachete UDP de 1518/64 octeți: 16 Gbps • Trafic IPSec VPN (AES 256 SHA1): 12 Gbps • Trafic IPS pentru pachete UDP de 512 octeți: 1 Gbps • Trafic antivirus: 350 Mbps • Număr de tunele IPSec VPN concurente: 10000 • Număr de clienţi VPN concurenți: 20000 • Număr de sesiuni concurente: 1000000 • Număr de sesiuni noi pe secundă: 25000 • Număr de politici de securitate: 100000 • Număr de instanțe virtuale (mașini virtuale): 10 • Număr de utilizatori nelimitați • Consum mediu de putere: maxim 225W

Funcționalități generale	• Echipament integrat de securitate cu funcționalități simultane de:
	  • Firewall și firewall la nivel de aplicație de tip stateful - detectarea/blocarea aplicațiilor software
	  • Protecție antivirus
	  • Criptare de date: IPSec VPN și SSL VPN
	  • QoS și Traffic Shaping
	  • Detecția și prevenirea intruziunilor – IDS/IPS
	  • Scanare și filtrare WEB – Web Inspection/Filter
	  • Protecție antispam
	  • Protecție împotriva scurgerii de informații confidențiale
	• Toate funcționalitățile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum și platforma hardware trebuie să aparțină aceluiași producător
	• Certificări pentru producător și produs: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs pentru: Firewall, IPSec, SSL, Antivirus
	• Conformitate cu CE, FCC Class A Part 15, UL/CUL, VCCI
	• Toate funcțiile trebuie să fie disponibile standard, indiferent de număr de utilizatori sau IP-uri
	• Soluția trebuie să fie de tip echipament hardware cu sistem de operare propriu dedicat funcționalităților de securitate necesare

Funcționalități securitate	
Funcționalități firewall	• Funcționalități NAT, PAT și Transparent Bridge • Opțiune de a aplica NAT per politică • Suport VLAN Tagging 802.1Q • Autentificarea utilizatorilor pe grupuri • Suport VoIP SIP/H.323/SCCP și Transversal NAT • Funcționalitate proxy explicit • Suport WINS • Suport securitate VoIP (SIP Firewall/RTP Pinholing) • Suport IPv6 (NAT/mod Transparent) • Politici de securitate bazate pe identitatea utilizatorului/servicii folosite • Opțiune “Scheduling” pentru politicile de firewall • Certificare ICSA Labs (Enterprise Firewall)

Funcționalități VPN	• Suport PPTP, IPSec, L2TP + IPSec, SSL-VPN • Funcționalitate concentrator SSL-VPN (incluzând clienți iPhone) • Criptare DES, 3DES, AES • Autentificare SHA-1/SHA-256/MD5 • Suport pentru PPTP, L2TP, VPN Client Pass Through • Funcționalitate "Hub and Spoke" VPN • Autentificare IKE prin certificate X.509 (v1 & v2) • Suport IPSec NAT Transversal • Suport configurare IPSec automată • Funcționalitate IKE Dead Peer Detection • Suport pentru RSA SecureID • Suport Single-Sign-On pentru pentru book-mark-uri portal SSL-VPN • Funcționalitate Two-Factor Authentication pentru SSL-VPN • Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) • Suport tunele SSL în mod tunel și în mod portal • Funcționalități monitorizare tunele VPN • Certificare ICSA Labs (IPSec/SSL-TLS)
Funcționalități Antivirus	• Protecție anti-malware (virus, troian, worm, spyware) • Protocoale suportate: HTTP, SMTP, POP3 IMAP, FTP, IM (AIM, ICQ, YAHOO, MSN) • Blocare după nume/tip/dimensiune fișier • Suport scanare antivirus Flow-Based • Update-uri automate și împinse automat pe echipament • Suport pentru carantină a fișierelor infectate • Suport IPv6 • Opțiunea de a folosi diferite baze de date pentru semnături de viruși (în funcție de nivelul de securitate ales) • Certificare ICSA Labs (Gateway Antivirus)
Funcționalități filtrare trafic WEB	• Filtrare pentru protocoalele HTTP și HTTPS • Filtrare după categorii site-uri/URL • Funcționalitate de contorizare a timpului de acces pentru utilizatori • Blocare a conexiunilor în funcție de URL/cuvânt cheie sau expresie în conținutul paginilor web (HTTP) • Filtrare pentru Java Applet, Cookies, Active X (HTTP) • Filtrare după conținutul MIME Header (HTTP) • Suport IPv6
Funcționalități sistem de control al aplicațiilor	• Identificarea și controlul a peste 1000 de aplicații • Opțiune de Traffic-Shaping per aplicație • Control specific pentru aplicațiile de tip IM/P2P (incluzând AOL-IM, Yahoo, MSN, KaZaa, ICQ, Gnutella, BitTorrent, MySpace, WinNY, Skype, eDonkey, Facebook)

Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS)	• Protecție pentru peste 4000 de semnături de atac • Detectarea anomaliilor de protocol • Suport pentru semnături configurabile • Update-uri automate pentru semnături • Suport IPv6 • Protecție împotriva DoS
Funcționalități Antispam	• Scanare pentru SMTP, POP3, IMAP • Suport RBL/ORDBL • Inspecție header MIME • Filtrare după cuvinte cheie/expresie • Filtrare după Black/White List pentru adrese IP și e-mail • Update-uri automate și în timp real
Sistem de prevenire a scurgerii de informaţie (Data Leak Prevention)	• Identificare si controlul informaţiilor sensibile din trafic • Detectarea informaţiilor pe baza mai multor criterii configurabile (suport expresii RegEx) şi parametri ai fişierelor • Opţiuni de blocare/logare conexiunii in cazul detecţiei • Scanare pe protocoalele HTTP, SMTP, POP3, IMAP, FTP, IM(AIM, ICQ, YAHOO, MSN) • Suport pentru mai multe tipuri de fişiere • Suport pentru caractere internationale

Funcționalități sistem de verificare a stațiilor (Endpoint Control)	• Integrare cu o aplicație software pentru securitate ce rulează pe statii care să permită:
	  • Monitorizarea aplicațiilor instalate pe stații
	  • Restricționarea accesului în funcție de configurarea aplicației software de pe stații
	  • Scanarea pentru vulnerabilități a stațiilor

Funcționalități rețea	
Funcționalități rețelistică și rutare	• Suport pentru legături WAN multiple • Suport PPPoE și DHCP Client/Server • Rutare bazată pe politici • Rute statice • Rutare dinamică IPv4: RIP, OSPF, BGP, Multicast (PIM), IS-IS • Rutare dinamică IPv6: RIP, OSPF, BGP • Gruparea interfețelor în zone de securitate • Rutare între zonele de securitate • Suport VRRP și Link Failure Control • Suport sFlow • Suport VLAN Tagging (802.1q) • Rutare între VLAN-uri • Suport pentru IPv6 (Firewall, DNS, SIP) • Multi-Link Aggregation – 802.3ad • Posibilitate mapare (Binding) adrese IP – adrese MAC • Suport One-to-One NAT
Funcționalități Traffic Shaping	• Limitar/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicație și adresă IP • Suport pentru Differentiated Services (DiffServ) • Limitare a cotei de trafic (per adresă IP)
Suport domenii virtuale	1. Firewall/rutare per domeniu 2. Administrare separată per domeniu 3. Interfețe VLAN separate per domeniu 4. Politici de securitate per domeniu
Suport pentru centre de date – data center	• Balansare de trafic pentru servere • Multiplexare TCP • Suport WCCP
Funcționalități High Availability - HA	• Funcționare Active-Active, Active-Passive • Funcționalitate Stateful Failover (Firewall și VPN) • Detectare și notificare pentru echipament nefuncțional • Monitorizarea conexiunii la rețea • Funcționalitate Link Failover
Funcționalități de administrare, log-are, autentificare a utilizatorilor	
Funcționalități de administrare	• Administrare prin WEB UI (HTTP/HTTPS), Telnet, Secure Command Shell (SSH) și Command Line Interface (CLI) • Utilizatori/Administratori cu drepturi configurabile • Funcționalitate de export/import a configurației • Politică de control a parolelor

Funcționalități de log-are și monitorizare	• Funcționalitate de scanare a vulnerabilităților în rețea • Monitorizare grafică în timp real și istorică • Opțiune de păstrare a log-urilor pe memoria internă • Suport syslog/WELF • Suport SNMP • Notificare prin e-mail pentru alerte • Monitorizarea tunelelor VPN
Funcționalități de autentificare a utilizatorilor	1. Definire locală a utilizatorilor 2. Integrare cu Windows Active Directory (AD) 3. Integrare cu RADIUS/LDAP/TACACS+ 4. Suport Xauth prin RADIUS pentru IPSec VPN 5. Suport RSA SecureID 6. Suport pentru autentificarea grupurilor de utilizatori prin LDAP
Condiții de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz, 5A (Maxim)
Condiții de mediu	• Temperatură de operare: 0 - 40 grade Celsius

2. Echipament appliance tip EMAIL Firewall

Denumire	**Echipament integrat de protectie antispam si antivirus pentru traficul email cu capabilitati de operare in mod transparent(bridge), gateway(MTA) si server**
Configuraţie	• 2 x interfete 10/100/1000 Base T • 1 x interfete 10/100 Base T • 1 x port serial consola RJ-45
Caracteristici	• Domenii suportate: 50 • Politici pentru destinatari (per domeniu/per total): 60/300 • profile de protectie (per domeniu/per total): 50/60 • Numar de casute email locale(mod server): 200 • Capacitate HDD intern: 1 TB • Performante rutare mesaje email(de marime 3KB): 90000 mesaje/h • Performante scanare antispam pentru mesaje email(de marime 3KB): 85000 mesaje/h • Performante scanare antispam si antivirus pentru mesaje email(de marime 3KB): 77000 mesaje/h • Consum mediu de putere: maxim 56W

Functionalitati generale in modul de operare transparent, gateway(MTA) si server	- Configurare pentru domenii multiple - Suport High Availability - Configurabil ca SMTP Mail Gateway pentru servere mail existente - Rutare email pe baza de politici - Gestiune a stivei de email-uri(pentru mesaje netrimise, amanate sau nelivrabile) - Configurabil ca outbound mail relay - Politici granulare de detectie pentru spam si virusi - Optiuni de configurare folosind adrese email, adrese IP si domenii - Configurare functionalitati antispam si antivirus pentru utilizatori folosind atribute LDAP per politica(domeniu) - Rutare email folosind LDAP - Optiune de acces a carantinei email prin WebMail si POP3 - Trimitere sumar zilnic al carantinei - Arhivare pe baza de politici a mesajelor inbound si outbound cu optiune de remote backup - Autentificare SMTP prin LDAP, RADIUS, POP3 sau IMAP - Suport whitelist-uri per user - Suport SNMP - Functionalitate Sender Reputation List locala pe baza: - numarului de virusi trimisi - numarului de mesaje spam trimise - numarul de destinari inexistenti - Suport Dynamic DNS (DDNS) - Suport Greylist - Suport Regex pentru identificarea pattern-urilor - Suport Sender Policy Framework (SPF) - Suport DomainKeys - Suport DomainKeys Identified Mail (DKIM) - Blocarea mesjelor fragmentate - Suport Virtual Host utilizand grupuri de adrese IP ca destinatie sau expeditor
Functionalitati specifice modului de operare server	• Suport pentru protocaolele POP3, SMTP, and IMAP • Suport pentru SMTP over SSL • Politici de utilizare a capcitatii de socare pentru casutele utilizatorilor • Acces securizat pentru utilizatori • Optiuni de configurare folosind utilizatorul, grupul de utilizatori si alias-uri • Autentificare locala si prin LDAP • Optiunea Bulk Folder pentru spamuri
Functionalitati High Availability (HA)	• Configurabil in modul de operare transparent, gateway(MTA) si server • Configurare activ-pasiv sau in distributie de sarcina • Sincronizare a stivei de emailuri si a carantinei • Stateful Failover • Link Failover • Link Status Monitor • Detectie si notificare a problemelor de functionare

Functionalitati protectie Antivirus / Antispyware	• Scanare SMTP pentru virusi cu suport pentru atasamente comprimate si arhive • Carantina pentru fisiere infectate • Notificare prin inlcouirea continutului email • Blocare dupa tipa fisier • Filtrare atasamente
Functionalitati de protectie impotriva atacurilor	• Mecanisme de protectie impotriva atacurilor de tip DoS(Mail Bombing), Recipient Address Attack, Forged Sender Address. • Mecanisme pentru: - Email Rate Limiting - Reverse DNS Check (Anti-Spoofing)
Functionalitati de criptare a transferului de date	• Suport Identity-based Encryption(IBE) pentru livrarea Push/Pull a mesajelor criptate • Suport S/MIME Support pentru criptare Gateway-Gateway • Support pentru protocoale de criptare puternice (HTTPS, SMTPS, SSH, IMAPS si POP3S)
Functionalitati Antispam	I. Filtrare inbound si outbound II. Filtre antispam cu reguli euristice III. Updatare dinamica pentru reguli euristice IV. Filtrare atasamente/continut V. Insspectie a header-ului mesajelor email VI. Filtrare folosind metode statistice Bayesian VII. Suport Spam URI Real-Time Blocklists (SURBL) VIII. Filtrare supa cuvinte IX. Carantina si etichetare pentru mesaje spam X. Gestiune pentru mesaje spam (Accept, Relay, Reject sau Discard) bazata pe Email SHASH Spam Checksum Blocklist XI. Scanare anatispam cu analiza de imagini XII. Scanare PDF / imagine PDF XIII. Suport pentru Black/White List-uri globale si configurabile de catre utilizatori XIV. Suport Real-Time Black Listed (RBL) XV. Suport Forged IP XVI. Suport Greylist Checking
Functionalitati de gestiune, logare si raportare	• Statistici in timp real • Conturi de administrare ierarhizate • Optiune de inspectie a carantinei • Creeare automata de raporturi in format PDF • Logare a modificarilor configuratiei • Logare activitate antispam • Logare activitate antivirus • Suport pentru server Syslog extern sau local • Suport pentru server stocare extern sau local, inclusiv dispozitive iSCSI • Alertare pentru evenimente critice • Functionalitati de creeare a rapoartelor, inclusiv rapoarte programate
Condiții de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz, 1.5A (Maxim)

Condiții de mediu	• Temperatură de operare: 0 - 40 grade Celsius

3. Echipament de logging

Denumire	**Echipament integrat destinat colectării de log-uri ale echipamentelor de rețea cu capabilități de analiză și raportare a datelor recepționate**
Configuraţie	• 4 interfețe 10/100/1000 Base T • 1 port consolă RJ45

Caracteristici	• Viteză de procesare: 1000 log/sec • Rată de colectare log-uri: 4 Mbps • Număr de echipamente monitorizate: 2000 • Capacitate HDD intern: 1TB (capacitate pana la 4TB) • Suport RAID 0, 1, 10 • Consum mediu de putere: maxim 189W
Funcționalități generale	• Administrare prin WEB UI (HTTP/HTTPS), Telnet, Secure Command Shell (SSH), Command Line Interface (CLI) • Administrare bazată pe profile • Comunicare criptată și autentificare cu echipamentele monitorizate • Alertare prin e-mail • Interpretare trap-uri SNMP • Suport mesaje în format de tip Syslog • Suport interconectare cu un sistem extern de depozitare a log-urilor de tip NAS – Network Attached Storage • Configurare setări de bază sistem • Suport din interfața grafică de tip “online help” • Gestiune listă de echipamente monitorizate: adăugare, modificare, ștergere • Vizualizare echipamente monitorizate pe baza apartenenței la un grup predefinit • Vizualizare încercări eșuate de interconectare a echipamentelor cu sistemul de colectare de log-uri • Configurare și vizualizare alerte referitor la starea echipamentului • Vizualizare status conexiune cu echipament de management centralizat • Vizualizare informații sistem/resurse • Vizualizare perioadă valabilitate licențe cu alertare prealabilă expirării acestora • Vizualizare statistici funcționare echipament din punct de vedere hardware • Vizualizare istorie funcționare • Vizualizare informații sesiuni stabilite cu echipamentele monitorizate • Funcționalitate de export/import a configurației • Opțiune de incărcare setări din fabrică • Opțiune de formatare discuri • Opțiune upgrade firmware • Soluția trebuie să fie de tip echipament hardware cu sistem de operare propriu dedicat funcționalităților de colectare, analiză și raportare cu sistem de operare propriu
Funcționalități arhivare a traficului transferat prin echipamentele monitorizate	• Arhivare a traficului pe baza funcționalității de prevenire a scurgerii de informații (DLP) prezentă pe echipamentele monitorizate • Arhivare a traficului de tip - HTTP (Web URLs), FTP (nume fișier), E-mail (text), Instant Messaging (Text) - transferat prin echipamentele monitorizate • Vizualizare arhivă după tipul de trafic • Arhivarea integrală a traficului • Arhivare sumară a traficului (fără arhivarea conținutului trasferat) • Posibilitatea de a aplica filtre de vizualizare pe conținutul arhivat

Funcționalități de analiză rețea	• Vizualizare în timp real al traficului transferat de echipamentele monitorizate • Vizualizare a istoricului traficului • Posibilitatea definirii filtrelor de vizualizare

Funcționalități analiză și raportare	• Generare rapoarte în următoarele formate: HTML, PDF, MS Word, Text, MHT, XML
	• Opțiune de trimitere/upload a rapoartelor generate prin e-mail, FTP, SFTP, SCP
	• Opțiune de selecție a log-urilor utilizate pentru generarea de rapoarte
	• Raportare bazată pe profile
	• Vizualizare rezumate evenimente de securitate
	• Existența unor modele de rapoarte predefinite
	• Posibilitatea generării de rapoarte personalizate
	• Posibilitatea generării de grafice personalizate în rapoartele generate
	• Tipuri de rapoarte:
	  • Atacuri: după echipament, după oră/zi, după categorie, după topul surselor
	  • Viruși: topul virușilor detectați, viruși detectați per protocol
	  • Evenimente: după firewall, după numărul de evenimente declanșate pe zi
	  • Utilizare e-mail: topul e-mail-urilor după user, atât e-mail-urile care vin cât și cele care ies
	  • Utilizare Web: top utilizatori Web, top site-uri blocate, top clienți
	  • Utilizare bandă: top utilizatori bandă, după utilizarea benzii pe zi/oră, după utilizarea benzii per protocol
	  • Protocoale: top protocoale, top utilizatori FTP, top utilizatori Telnet

Funcționalități carantină centralizată	• Arhivarea fișierelor infectate într-o zonă de tip carantină • Configurare setări carantină • Vizualizare listă fișiere în carantină • Control eliberare carantină automatizată

Funcționalități analiză aprofundată a datelor	• Înregistrarea activității după nume utilizator, e-mail, adresă sau nume Instant Messaging
	• Suport pentru filtrarea WEB pe categorii și vizualizarea site-urilor blocate pentru fiecare utilizator
	• Parametrii configurabili pentru fiecare raport:
	  • Profile
	  • Echipamente
	  • Raza de activitate
	  • Tipuri
	  • Format
	  • Program
	  • Rezultat
	• Generarea de raporte personalizate
	• Generarea de rapoarte la cerere
	• Funcționalități de parcurgere rapoarte

Funcționalități explorare log-uri și vizualizare în timp real a log-urilor	• Vizualizare/căutare/management log-uri
	• Vizualizare log-uri în timp real printr-o interfață de tip Web
	• Vizualizare istoric log-uri
	• Vizualizari personalizate log-uri și filtrare informații afișate
	• Căutare în log-uri după cuvinte cheie
	• Vizualizare trafic Web, e-mail, FTP, IM sau P2P
	• Vizualizare rezumate trafic generate în urma analizei log-urilor generate de echipamentele monitorizate
	• Rapoartele de trafic trebuie să conțină:
	  • Evenimente (audit de către admin)
	  • Viruși detectați
	  • Atacuri (de tip IPS)
	  • Filtrare conținut Web
	  • Filtrare e-mail-uri
	  • Conținut trafic (Web, e-mail, IM)

Funcționalități scanare vulnerabilități	• Configurare sarcini scanare vulnerabilități • Rulare sarcini scanare vulnerabilități • Vizualizare rezumate rapoarte • Vizualizare rapoarte detaliate • Compatibilitate cu terminologia CVE • Scanare și raportare PCI DSS
Condiții de alimentare	- Alimentare curent alternativ 100-240V, 50-60 Hz, 7A (Maxim)
Condiții de mediu	• Temperatură de operare: 0 - 40 grade Celsius

4. Statie de lucru mobila

Procesor	Intel Core i3
Memorie HDD	4 GB RAM extensibil la 8GB RAM minim 500GB @ 7200 RPM
Placa grafica Display	onboard 14'' TFT LCD cu LED rezolutie minima 1366 x 768
DVD Multimedia	DVD±RW Webcam, microfon, boxe stereo incorporate
Retelistica	Wireless B/G/N, retea 10/100/1000, bluetooth 3.0, modem

Porturi	3x USB 2.0 (1x eSATA) 1x VGA 1x DisplayPort 1x RJ-45 1x Microfon 1x Express Card 34 mm 1x Cititor carduri 4v1 (MMC, SD, SDHC, SDXC)
Baterie	minim 6 celule Li-Ion
Sistem operare preinstalat	Microsoft Windows 7 Professional 64 bit
Software preinstalat	- solutie pentru recuperarea datelor - securitatea datelor si criptare informatii - actualizare drivere

5. Software replicare

Nr. Crt.	*Cerinte*
1	replicare continua a datelor intre mediul de productie si cel de backup pe infrastructura existenta
2	replicarea setarilor de securitate din sistemul de fisiere NTFS
3	protectie in timp real pentru sistemul de operare si/sau pentru aplicatiile instalate
4	instalare pe infrastructura existenta fara a afecta performantele serverelor
5	protectie pentru intregul sistem cu posibilitate de failover automat sau manual in caz de incident
6	timp de restaurare a sistemului de operare si / sau aplicatiilor de maxim 10 minute
7	solutia sa permita recuperarea pe hardware diferit sau in mediu virtual
8	suport pentru protejarea aplicatiilor MS SQL Server, MS Exchange, Oracle, Sharepoint, Lotus Domino, Blackberry Enterprise Server si altele
9	integrare nativa cu Microsoft VSS cu posibilitatea de a avea pana la 64 de imagini (snapshot) si recuperarea acestora pe medii fizice sau virtuale
10	fara limitarea distantei intre mediul de productie si cel de backup
11	suport pentru replicare din masini virtuale instalate pe Microsoft Hyper-V catre masini virtuale instalate pe VMware vSphere
12	solutie certificata Microsoft
13	posibilitate instalare automatizata de la distanta printr-o interfata proprietara centralizata de administrare
14	validare setari si posibilitate de auto-fix
15	raportare centralizata pentru intreaga solutie
16	posibilitate compresie date transferate, definire intervale orare de transmitere date si posibilitate alocare si / sau limitare a latimii de banda in intervale orare
17	utilitar integrat pentru estimarea latimii de banda necesare in mediul de productie
18	notificari e-mail, integrare cu Microsoft MOM
19	suport pentru Microsoft Hyper-V si VMware vSphere
20	posibilitate replicare si failover fizic - fizic / fizic - virtual / virtual - fizic / virtual – virtual
21	posibilitatea generarii automate a masinii virtuale pentru recovery pe baza unor parametri presetati
22	suport pentru Microsoft Cluster
23	posibilitate failover a unui Cluster Microsoft catre un singur server
24	posibilitatea salvarii unei imagini pe un mediu intermediar cu optiunea de a recupera aceasta imagine catre mediu fizic sau virtual
25	posibilitatea replicarii one-to-one, one-to-many, many-to-one

Cerinte minime obligatorii:

- ✓ Certificari pentru platforme Microsoft Windows Server (MCSE) sau echivalent
- ✓ Certificari emise de catre producatorul solutiei de replicare
- ✓ Certificari emise de furnizorul solutiei de securitate
- ✓ Training autorizat pe platforma de securitate sustinut de catre o persoana certificata de producator. Trainingul va fi efectuat pentru doua persoane din partea achizitorului.
- ✓ Se solicită prezentarea autorizaţiei de comercializare, instalare, suport şi asistenţă tehnică de la producător pentru toate produsele software şi hardware ce vor fi livrate, care să conţina cel putin numele procedurii de achiziţie, numele operatorului economic autorizat să presteze serviciile solicitate, numele Autoritatii Contractante, data emiterii.
- ✓ Livrare, Instalare si punere in fuctiune maxim 20 zile