CONSILIUL JUDEŢEAN TIMIŞ
Direcţia Generală Economică, Informatizare
Compartimentul Informatică

Nr. 12301 data: 02.07.2018

CAIET DE SARCINI
pentru
"Echipament de rețea protecție "next generation firewall" cu licenţă pentru 3 ani"

1. **Caracteristici tehnice minimale pentru – achiziția de *"Echipament de rețea protecție "next generation firewall" cu licenţă pentru 3 ani" pentru rețeaua informatică a C.J. Timiș".***

Nr. Crt.	Specificaţii tehnice impuse prin caietul de sarcini
1	***Echipament de rețea protecție "next generation firewall" cu licenţă pentru 3 ani" = 1 buc.***
1.1	➢ **Descriere generala**: Echipament integrat de protectie in retea, cu capabilitati de protectie antivirus si prevenirea intruziunilor, destinat folosirii ca o solutie de securitate unificata. ➢ **Specificatii hardware:** ○ 4 x GE RJ45 ○ 4 x sloturi GE SFP/ 4 x 10 Gigabit SFP+ ○ 1 x port micro USB; 1 x port USB ○ Port RJ-45 consola ○ 1 x 10/100/1000 Ethernet management out of band ○ Storage intern 240GB SSD pentru loguri ➢ **Performanta minima a sistemului:** ○ Throughput firewall cu identificare aplicatie: 900 Mbps ○ Throughput firewall (IPS+AV+IDS+Data filtering, activate simultan): 600 Mbps ○ Throughput IPSec VPN: 400 Mbps ○ Numar tunele SSL-VPN si IPSec: 1000 ○ Sesiuni concurente SSL Inspection: 12500 ○ Tunele IPSec VPN Gateway-to-Gateway: 2000 ○ Tunele IPSec VPN Client-to-Gateway: 1000 ○ Sesiuni concurente (TCP): 130000 ○ Sesiuni noi/sec (TCP): 8000 ○ Politici firewall: 1500 ○ Suport identificare utilizatori: 100.000 ○ Configuratii redundante posibile: Activ/Activ, Activ/Pasiv cu full state failover ○ ARP table: minim 3000 intrari ➢ **Parametrii echipament:** ○ Consum maxim 200W ○ Sursa alimentare redundanta, inclusa ○ Montabil in rack maxim 1U

- **Protocoale si standarde:**

  Servicii de retea

  - Rutare/Retea:
    - Suport WAN pentru configuratii cu furnizori de internet multiplii
    - Client/Server DHCP
    - Policy-based routing
    - Rutare dinamica Ipv4/Ipv6-RIP ,OSPF, BGP
    - Minim 5000 rute statice IPv4
    - Suport routere multiple virtuale cu tabele de rutare separate
    - Rutare intre zone
    - VLAN Tagging(802.1q)
    - Rutare intre VLAN-uri
    - Multi-link aggregation (802.3ad)
    - Suport IPv6
    - Rutare multicast: PIM-SM, PIM-SSM, IGMP – v1,2,3
    - Mod interfete: sniffer, agregare port, loopback, transparent (fara MAC address), layer 2, layer 3
  - Traffic Shaping:
    - Policy-based
    - Suport DiffServ
    - Banda Garantata/Maxima/Prioritara
    - Shaping per-IP,per-Account, per zona de securitate, per grup utilizatori, per aplicatie, per grup de aplicatii, per politica de securitate
  - Domenii Virtuale:
    - Minim 5 instante de rutare
    - Minim 30 zone de securitate simultane ce pot contine interfete in moduri de functionare diverse (L2,L3, sniffer, transparent)
    - Interfete VLAN separate
  - High Availability:
    - Activ/Activ cu suport pentru rutare asimetrica
    - Activ/Pasiv cu Statefull Failover
    - Link status monitor; host status monitor
    - Link failover
    - Load Balancing pentru rutare WAN

- ***Servicii de Securitate***

  - Echipamentul trebuie sa actioneze in conformitate cu principiul „Minimal Privilege", adica sa blocheze toate aplicatiile, indiferent de portul TCP/IP, cu exceptia celor permise explicit si pentru care sunt indicate normele de politica de securitate.
  - Echipamentul trebuie sa permita crearea manuala de semnaturi pentru aplicatii aditionale, direct pe dispozitiv in interfaaa de administrare, fara a necesita instrumente externe sau implicarea producătorului.
  - Echipamentul trebuie sa permita definirea de actiuni de tip blocare sau continuare pentru prevenirea atacurilor de tip «drive by download» prin afisarea unei pagini care informeaza utilizatorul si eventual permite continuarea download-ului dupa acceptul utilizatorului.
  - Echipamentul trebuie sa asigure inspectia traficului criptat SSL inclusiv pentru comunicatii ce nu folosesc protocol HTTP, si sa realizeze inspectia traficului decriptat pentru detectie Antivirus, Anti-spyware, fisiere de date.

- Echipamentul trebuie sa poata fi configurat cu un set de politici de decriptare si inspectie specifica a traficului SSL separat de politicile de securitate a traficului decriptat.
- Echipamentul trebuie sa permita configurarea profilelor de identificare IPS/IDS in mod specific pentru fiecare regula de securitate in parte. Nu se accepta ca scanarea IPS/IDS sa se realizeze doar la nivelul intregului echipament sau doar pentru interfete specifice.

Firewall:

- NAT, Transparent
- Rutare dinamica-RIP,OSPF,BGP,Multicast
- Policy-based NAT
- Politici NAT separate de configuratii de rutare
- Domenii Virtuale (NAT/Transparent)
- VLAN Tagging (802.1q)
- NAT ALG pentru FTP, MGCP, MySQL, Oracle, RPC, RTSP, SCCP, SIP
- Profile granulare de protectie per-policy

VPN:

- IPSec,SSL
- Suport criptare 3DES, AES (128,192,256)
- Autentificare SHA-1 / MD5/SHA-256/SHA-384/ SHA-512
- PPTP,L2TP,VPN Client pass through
- Suport VPN "Hub and Spoke"
- Autentificare IKE cu Certificate (v1 si v2) si preshared key
- IPSec NAT Traversal

Prevenirea Intruziunilor:

- Suport anomalii de protocoale
- Suport semnaturi definite de utilizator
- Suport Ipv6
- IDS sniffer mode
- Logare a pachetelor

Antivirus:

- Suport Anti-spyware
- Suport pentru sandboxing
- HTTP/HTTPS; POP/POP3S; SMTP/SMTPS; IMAP/IMAPS; FTP; SMB
- Blocarea fisierelor in functie de tip sau dimensiune
- Suport IPv6
- Reguli distincte de blocare a fisierelor per aplicatie, indiferent de port TCP/IP, diferentiat upload/download, definite in cadrul regulilor de securitate firewall.

Filtrare URL:

- Baza de date se actualizeaza cu URL-uri declarate malitioase la maxim fiecare 30 minute
- Echipamentul trebuie sa asigure, fara componente hardware sau software aditionale, filtrarea accesului Web in functie de categorii de continut pentru servere HTTP. Baza de date cu URL-uri si categoriile de continut trebuie sa fie actualizata regulat in mod automat (pe baza de subscriptie la serviciul de actualizare al producatorului echipamentului) si trebuie sa includa cel putin 20 de milioane de intrari URL.

➢ **Management:**

- Administrare:
  - Consola, SSH, HTTPS, CLI
  - Permite configurarea tuturor functionalitatilor fara software adiacent de management

	• Utilizatori/Administratori cu drepturi configurabile • Syslog, SNMP, log-uri interne, grafice, notificari e-mail • Capabilitate de export de loguri filtrate pe baza regulilor definite de administrator. • Capabilitate de export diferentiat pentru fiecare regula de securitate in parte • Capabilitate de management complet prin API de tip web/xml • Backup: configuratia trebuie sa se poata salva si restaura sub forma unui fisier text/xml o Autentificare: • Baza de date locala • Integrare Active Directory • Integrare LDAP/Radius/TACACS+ • Integrare directa cu Microsoft AD, RADIUS, Syslog, Web API pentru identificarea utilizatorilor din LDAP/AD cu adresa IP • Capabilitate de a forta autentificare multifactor pentru accesul catre o zona sau un grup de servere o Nu se acceptă echipamente de tip "cloud-based" ➢ **Subscripţie (licenţiere):** o Fara limitare a numarului de adrese IP prin subscripţie (licenţiere) o Fara limitare a numarului de statii de administrare prin subscripţie (licenţiere) o Fara limitare pentru suport IPv6 prin subscripţie (licenţiere) o Subscripţie (icenţiere) pentru activarea actualizărilor serviciilor IDS/IPS, Prevenirea Intruziunilor si filtrare URL: 36 luni o Interfetele sa fie active la viteza maxima o Echipamentul trebuie sa continue sa funcţioneze dupa expirarea acestor subscripţii (licenţiere). ➢ **Servicii instalare si configurare:** o Instalare echipament in locatie conform specificatiilor beneficiarului o Conectare ethernet o Configurare IP management si plan adresare o Configurare lista de acces la internet o Configurare a serviciului antimalware si URL filtering conform cerintelor beneficiarului o Testare solutie securitate: URL-filtering si anti-malware ➢ Testare solutie securitate prin teste specifice (penetration test, filtrare URL, antivirus) ➢ Realizare si prezentare documentatie: conectivitate, planuri adresare, credentiale acces echipament;
1.2	**Conditii privind conformitatea cu standardele relevante:** Standard de calitate ISO 9001, (sau echivalent) pentru producator
1.3	**Conditii de garantie şi post garantie:** *Perioada de garanţie* ➢ **Garantie şi suport:** o Garanţie echipament: minim 36 luni o Subscripţie (licenţiere) semnături: 36 luni *Garanţia echipamentului cade în răspunderea furnizorului pe toată perioada de garanţie definită în ofertă;* *Furnizorul trebuie să intervină pentru constatarea unei defecţiuni în termen de 24 ore de la sesizare şi remedierea defecţiunii în maxim 5 zile lucrătoare de la data constatării acesteia;* *În cazul în care remedierea defecţiunilor nu se poate realiza, în termen de maxim 30 de zile echipamentul va fi înlocuit cu unul nou, cu o configuraţie echivalentă/superioară faţă de cea livrată.*

1.4	**Certificari necesare:** o Personal certificat de producator pentru configurarea și instalarea echipamentului;
2.	**Subscripție (licențiere) update pe 3 ani**
2.1	➢ Subscripție (licențiere) pe 3 ani pentru prevenirea amenințărilor (Threat prevention subscription 3 years)
2.2	➢ Subscripție (licențiere) pe 3 ani pentru filtrarea adreselor de internet (URL filtering subscription 3 years)

Alte cerinţe:

- Caracteristicile tehnice specificate în caietul de sarcini vor fi minime şi obligatorii;
- Pentru calitatea echipamentului ofertantul va remite documente valabile emise sau obţinute de producător.

Director General,
Direcţia Generală Economică, Informatizare
Marcel MARCU

Compartiment Informatică,

Viorel IEȘAN – Consilier Superior
Gabriel ROȘU – Consilier Superior
Adrian TUCE – Consilier Principal