CAIET DE SARCINI

Achiziționarea Cluster NGFW (Next Generation Firewall) pentru zona de border cu suport inclus pentru o perioada de 5 ani

Cuprins

CAIET DE SARCINI

1. Descrierea stării prezente

Managementul companiilor din zilele noastre se bazează pe informații corecte care sunt condiționate de utilizarea tehnologiei moderne de comunicare. Sistemul de informații trebuie să fie disponibil 24 ore pe zi, 7 zile pe săptămână, orice cădere a sistemului putând avea repercusiuni grave asupra activității societății. Prin urmare activitatea societății depinde de puterea sistemului de informații, care trebuie protejat de un sistem de securitate eficient și flexibil.

În prezent soluția de securitate IT este formată dintr-un cluster de două echipamente de tip firewall (Fortigate NGFW) cu suport care expiră în decembrie anul acesta. Vechimea soluției de securitate este de 3 ani, fapt ce impune înlocuirea acesteia cu echipamente de generație nouă, care să asigure un volum de trafic de date mai mare și să fie adaptată la cerințele actuale în materie de securitate IT.

2. Prezentare generală a lucrării

Achiziția de echipamente pentru asigurarea securității infrastructurii IT.

Soluția conține :

- Cluster de echipamente hardware firewall NGFW pentru zona de border (delimitează rețeaua internă Conpet de internet), filtrează traficul din rețeaua Conpet spre internet și invers.
- Module SFP proprietare pentru asigurarea conectivității cu echipamentele din rețeaua internă Conpet.
- Licențele software și suportul necesar activării și funcționarii modulelor din firewall.

3. Cerințe tehnice

Echipamentele firewall trebuie să fie de tip hardware, să ofere performanțe superioare soluției de securitate actuale și să combine toate modulele de securitate (Antivirus, WebFilter, DNS Filter, Application Control, Intrusion Prevention , Anti-Spam, SSL/SSH inspection, VPN etc) într-un singur appliance pentru o mai bună administrare a soluției (management centralizat).

Echipamentele de tip firewall trebuie să fie de tip NGFW (Next Generation Threat Protection/Prevention) și să asigure protecție dar și vizibilitate la nivel de rețea Layer 7.

Echipamentele trebuie să dispună de surse de alimentare redundante. Conectica (modulele SFP) trebuie să fie proprietară pentru asigurarea compatibilității între echipamente.

3.1 Specificații firewall NGFW 601E :

IPS Throughput	10 Gbps
NGFW Throughput	9.5 Gbps
Threat Protection Throughput	7 Gbps
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps
Firewall Latency (64 byte, UDP)	2 µs
Firewall Throughput (Packet per Second)	40.5 Mpps
Concurrent Sessions (TCP)	8 Million
New Sessions/Second (TCP)	450,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	20 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	7 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000
SSL Inspection Throughput (IPS, avg. HTTPS)	8 Gbps
SSL Inspection CPS (IPS, avg. HTTPS	5,500

SSL Inspection Concurrent Session (IPS, avg. HTTPS)	800,000
Application Control Throughput (HTTP 64K)	15 Gbps
CAPWAP Throughput (HTTP 64K)	18 Gbps
Virtual Domains (Default / Maximum)	10/10
Maximum Number of FortiSwitches Supported	64
Maximum Number of FortiAPs (Total / Tunnel)	1,024 / 512
Maximum Number of FortiTokens	5000
Maximum Number of Registered FortiClients	2000
High Availability Configurations	Active-Active, Active-Passive, Clustering
Local Storage	2x 240 GB SSD
Redundant Power Supplies (Hot Swappable)	**Yes**

3.2 Conectică Fortinet

FG-TRAN-SX - **8 bucăți**

FG-TRAN-SX	
Protocol Standard	1000Base-SX
IEEE Standard	802.3z
Module Type	SFP
Data Link Rate for Ethernet	1.25 Gbps
Transmission Range	220 m / 500 m
Media	MM
Wavelength (nm)	850
Connector Type	Duplex LC
Power Dissipation	< 800 mw
Operating Temperature Range	0–70°C
Hot Plug	Yes
Serial ID PROM	Yes
Digital Monitoring	No
Auto Negotiation	Yes
Link Status	Yes

3.3 Suport tehnic Fortinet

Fortinet oferă 4 tipuri de suport :

1. 360 Protection
2. Enterprise Protection
3. **UTM**
4. Threat Protection.

Suportul tehnic care se va achiziționa trebuie să fie pe o perioada de 5 ani și să includă următoarele : acces la update-uri de firmware/IOS, update la baza de data AV & IPS (Antivirus si Intrusion Prevention System), Semnături Application Control, Web Filtering, Anti-Spam Filtering, FortiCare Support (Hardware Version – return to factory, Enhanced Support – 8x5 support). Toate acestea sunt incluse în suportul tehnic de tip **UTM**.

Suport UTM	
FortiCare	24x7
FortiGuard App Control Service	Da
FortiGuard IPS Service	Da
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	Da
FortiGuard Web Filtering Service	Da
FortiGuard Antispam Service	Da
Perioada	**5 ani – incepand cu luna Decembrie 2020**

4. Servicii

Prestatorul trebuie să furnizeze toate bunurile și serviciile descrise în acest document și trebuie să își asume responsabilitatea completă pentru livrarea cantității corecte și a licențelor necesare funcționării corespunzătoare a modulelor din firewall.

5. Livrarea

Livrarea echipamentelor, licențelor și altor accesorii se va face la Sediul Dispecerat Central din Ploiești str. Anul 1848, nr.1-3 in maxim 45 zile de la semnarea contractului.

6. Garanție

Prestatorul trebuie să furnizeze Beneficiarului garanție comercială conform suportului achiziționat (5 ani) de la data semnării procesului verbal de recepție pentru toate licențele și echipamentele livrate.

Întocmit,

Șef Birou Infrastructură IT

Ing. Costin Florescu

Administrator Rețea

Ing. Lucian Gheorghe

Avizat,

Șef Dep. Dezvoltare Mentenanta

Ing. Dan Buzatu

Șef Serviciu IT

ec. Razvan pop