# Caiet de sarcini – firewll hardware

# Specificații tehnice și funcționale

## Mod de prezentare

Sistemul intern trebuie sa fie protejat de o componenta firewall care limiteaza traficul prin politici stricte de access, pentru functionarea in conditii de securitate ridicata a aplicatiilor.

Modelul de securitate va fi unul complet integrat bazat pe politici si reguli pentru informatii si date cat si pentru utilizatori.

Asigurarea securitatii logice se va realiza prin implementarea echipamentelor hardware firewall.

## Cerinte tehnice generale

1. Interfete:

* 5 porturi Fast Ethernet 10/100 BaseT, upgradabil la 2 porturi Gigabit Ethernet 10/100/1000 BaseT + 3 porturi Fast Ethernet 10/100 BaseT ;
* Suport pentru minim 50 VLAN –uri;
* minim doua porturi USB 2.0;
* 1 x Port consola;
* 1 x Port auxiliar pentru administrare de la distanta;.

1. Performante:

* Capacitatea de procesare la nivel de firewall: minim 300 Mbps;
* Capacitatea de procesare la nivel de trafic VPN: minim 170 Mbps;
* IPS (Intrusion Prevention System) – Da;
* Conexiuni noi pe secunda - Minim 10000.
* Numar minim de utilizatori – Nerestrictionat.

1. Functionalitate UTM:

* Anti-spyware;
* Anti-spam.

1. Protocoale de rutare suportate: RIP, OSPF;.
2. Filtrare - Filtrarea traficului la nivel de protocol.
3. Dimensiuni - montabil in rack.

## Caracteristici

Arhitectura solutiei trebuie sa contina un nivel firewall hardware construit in tehnologie toleranta la defect hardware.

1. Acest nivel este dispus in punctul de acces dinspre reteaua externa (Internet) si asigura protectia traficului dispre exterior catre zona DMZ (nivelul de prezentare) si componenta de comunicatii.
2. Traficul dinspre zona DMZ catre zona de aplicatii se realizeaza prin intermediul unui al doilea echipament de tip firewall hardware.

Echipamentele firewall precum si ferma de servere componente ale sistemului vor inspecta conexiunile si traficul dinspre reteaua externa si vor bloca accesul neautorizat catre serviciile sistemului informatic integrat. Componenta de securitate contine si politicile de securitate, de autentificare si autorizare si acces la informatii cu consola de administrare centrala.

Componenta de securitate va contine un echipament hardware in arhitectura pentru punctul de conectivitate cu reteaua externa (Internet). Echipamentul hardware va contine si functie de detectie a atacurilor externe. Acest echipament asigura protectia traficului dinspre exterior catre nivelul de prezentare si componenta de comunicatii.

Componenta firewall si proxy va prelua cererile dinspre exterior, va aplica mecanismele si politicile de protectie configurate in sistem, iar apoi va transmite cererea catre ferma de servere.

De asemenea traficul dinspre nivelul de prezentare catre nivelul de aplicatii va fi verificat de catre echipamentul hardware firewall.