

Příloha 5 k Marketingovému průzkumu GDS

Výtisk č. 1

Počet listů: 2

## Požadavky na firewall

### L3 Firewall

Mezi základní prvky bezpečnosti se řadí stavový firewall. Firewall bude použit pro zabezpečení IP ekosystému, serverů pro zabezpečení hlasové komunikace a pro přestup do demilitarizované zóny (DMZ).

Pro zabezpečení funkcionality musí být použit Enterprise hardwarový firewall. V každém místě instalace firewallu se z důvodů zvýšení spolehlivosti požaduje dodání dvou zařízení (režim HA). Firewally musí umět pracovat v režimu Active/Active nebo Active/Passive.

Všechny instalované firewally budou centrálně spravované z jednotného rozhraní nainstalované v rámci dohledových systémů.

V rámci projektu musí být dodány dva typy zařízení:

- FW1 – firewall pro zabezpečení IP ekosystému a hlasové komunikace,
- FW2- firewall pro prostup do DMZ.

Dodaná zařízení ve funkci firewallu musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce.

### FW1- firewall pro zabezpečení IP ekosystému a hlasové komunikace

Pro zabezpečení prostupu do DMZ musí firewall splňovat následující parametry a služby:

- |                                                                                      |                               |
|--------------------------------------------------------------------------------------|-------------------------------|
| • Min. propustnost firewallu v UDP provozu při přenosu paketů o délce 64 – 1540 bytů | min 6 Gbps                    |
| • Min propustnost firewallu (paketů za sekundu)                                      | 10 Mpps                       |
| • Maximální zpoždění                                                                 | 2 μs                          |
| • Minimální počet současně otevřených spojení                                        | 2 miliónů spojení             |
| • Minimální počet nově otevřených spojení                                            | 50 000 spojení/s              |
| • Možnost rozšíření o IPS systém                                                     | Ano                           |
| • Minimální propustnost IPS sondy                                                    | 1 Gbps                        |
| • Rozhraní pro připojení do sítě                                                     | minimálně 8x1 Gbps            |
| • Napájení                                                                           | 230V                          |
| • Redundantní napájení                                                               | n+1                           |
| • Redundance FW                                                                      | Active/Active, Active/Passive |
| • Podpora 802.1Q VLAN                                                                |                               |
| • Podpora protokolu IPv6                                                             |                               |

Možnost vytváření samostatných (virtuálních) firewallů pro zabezpečení různých druhů provozu.

## FW2- firewall pro prostup do DMZ

Pro zabezpečení prostupu do DMZ musí firewall splňovat následující parametry a služby:

- Min. propustnost firewallu v UDP provozu při přenosu paketů o délce 64 – 1540 bytů min 20 Gbps
- Min propustnost firewallu (paketů za sekundu) 30 Mpps
- Maximální zpoždění 7  $\mu$ s
- Minimální počet současně otevřených spojení 6 miliónů spojení
- Minimální počet nově otevřených spojení 150 000 spojení/s
- Možnost rozšíření o IPS systém Ano
- Minimální propustnost IPS sondy 5 Gbps
- Minimální počet IP SEC tunelů pro propojení FW-FW 100
- Minimální počet IP SEC tunelů Klient-FW 20 000
- Rozhraní pro připojení do sítě minimálně 8x 1 Gbps  
minimálně 2x 10 Gbps
- Napájení 230V
- Redundantní napájení n+1
- Redundance FW Active/Active, Active/Passive
- Podpora 802.1Q VLAN
- Podpora protokolu IPv6

Možnost vytváření samostatných (virtuálních) firewallů pro zabezpečení různých druhů provozu.