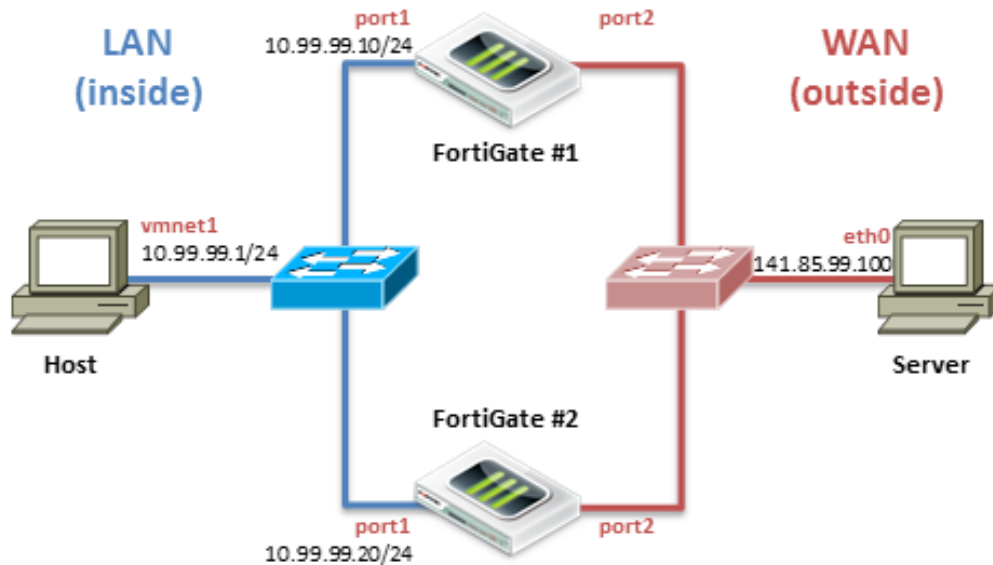


## Examen practic - FortiGate

### 1 Topologie



### 2 Observații

- Nu există doar un singur mod de rezolvare al exercițiilor . Orice soluție aplicată de voi ce respectă cerința și obține rezultatul dorit va fi punctată.
- Punctarea se face la nivel de subpunct.
- Singurele site-uri pe care aveți voie să le accesați sunt „docs.fortinet.com” și „ocw.cs.pub.ro”.
- Singura documentație pe care o puteți folosi o reprezintă slide-urile de curs.

### 3 Cerințe

1. [7p] Conectarea la echipamente și verificarea configurațiilor deja realizate.
  - a. [3p] Schimbați numele FortiGate-ului cu adresa 10.99.99.10 în **FortiGate1** și al FortiGate-ului cu adresa 10.99.99.20 în **FortiGate2**.
  - b. [4p] Pe **FortiGate1**, configurați un nou super\_admin numit *ADMIN\_EXAMEN* cu parola *sred*. Logați-vă cu noul administrator.
2. [18p] Rutare
  - a. [2p] Configurați următoarele adrese IP:
    - i. Pe **FortiGate1**, port2: 141.85.99.1/24
    - ii. Pe **FortiGate2**, port2: 141.85.99.2/24
  - b. [2p] Configurați următoarele interfețe de loopback:
    - i. Pe **FortiGate1**: Loopback0, 11.11.11.11/32
    - ii. Pe **FortiGate2**: Loopback0, 22.22.22.22/32
  - c. [5p] Configurați RIP pe cele două FortiGate-uri, astfel încât traficul dintre cele două Loopback-uri să treacă prin rețeaua externă (port2)
  - d. [5p] Configurați rute statice pe cele două FortiGate-uri, astfel încât traficul dintre cele două Loopback-uri să treacă prin rețeaua internă (port1)
  - e. [4p] Creați o singură politică de firewall pe fiecare FortiGate pentru a permite doar trafic ICMP între cele două Loopback-uri, prin interfețele **port1**. Testați folosind un ping extins.
3. [20p] Restricționarea traficului. Creați politici de trafic pe **FortiGate1** astfel încât următoarele cerințe să fie satisfăcute. Fiecare cerință trebuie să fie implementată fără a afecta cerințele anterioare.
  - a. [3p] Traficul ICMP către server nu trebuie să fie permis.
  - b. [4p] Traficul SSH de la **Host** (10.99.99.1) către **Server** (141.85.99.100) trebuie să fie permis.
  - c. [10p] Traficul HTTP de la **Host** (10.99.99.1) către **Server** (141.85.99.100) trebuie permis, cu condiția ca utilizatorii să fie forțați să se autentifice înainte.
  - d. [3p] Modificați mesajul de login „Authentication required” în „Atenție: Se dă examen!!!”. **!!!Important:** Nu ștergeți tot conținutul, modificați doar textul respectiv.

4. [10p] Web filtering

- a. [6p] Pe **FortiGate1**, creați un filtru nou care blochează toate cererile GET care includ în URL șirurile de caractere „solutie”, „examen” sau „copiat”.
- b. [4p] Pe **FortiGate1**, modificați politica HTTP de la exercițiul 3 pentru a include și filtrul de URL-uri. Testați.