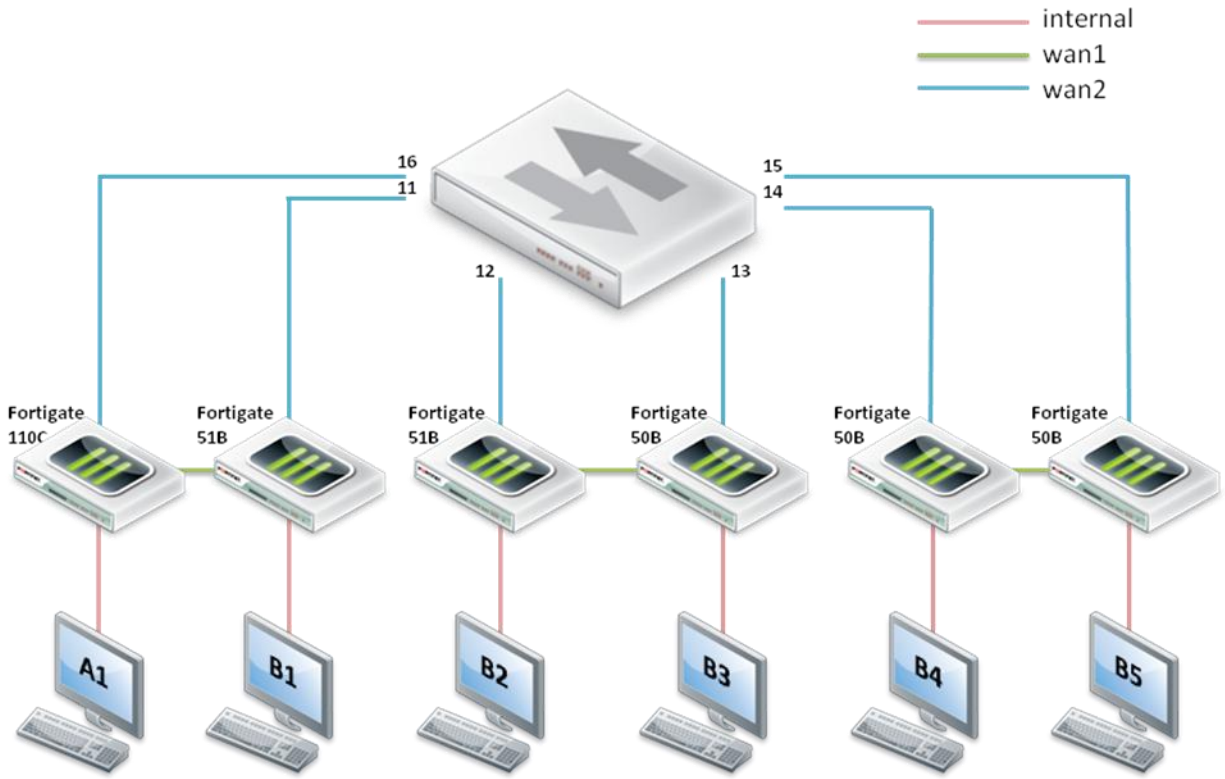
# MSSR Fortinet Lab 4 – Advanced firewall

## 1 Topologie




## 2 Cerințe

1. În cadrul acestui task, studenții vor configura echipamentul Fortinet pentru a permite accesul la Internet stației de lucru.

    a. Descărcați arhiva pentru laboratorul 1 de pe curs.cs.pub.ro, după care conectați stația existentă la portul din dreapta.

    b. Conectați-vă la unul din echipamentele din topologia de mai sus, în funcție de distribuția realizată de asistent, printr-un browser web, la IP-ul 192.168.1.99. Utilizatorul folosit este **admin,** și momentan nu este setată nicio parolă.

    c. Setați ceasul intern echipamentului Fortinet la ora exactă.

    d. Verificați că interfața WAN2 își va lua configurațiile prin DHCP.

e. [5p] Configurați o rută default pentru conectivitatea la Internet a echipamentului Fortinet, cu default-gateway 192.168.254.1. Verificați din consola Fortigate că echipamentul poate accesa Internetul.

f. [10p] Pe echipamentul Fortigate, configurați serviciul de DHCP pentru intervalul de adrese 192.168.1.1 – 192.168.1.100, excluzând IP-ul 192.168.1.99. Verificați că host-ul la care sunteți așezați își ia adresare prin DHCP.

g. [15p] Pentru accesul stației la Internet, creați o politică de firewall care să permită accesul oricărui tip de trafic din intern în afară, către WAN2. Echipamentul Fortinet va realiza NAT.

2. În cadrul acestui task, veți permite modificarea portului pe care se realizează inspecția pentru o aplicație și veți permite Active FTP.

   a. [20p] Descărcați și instalați pe stația de lucru FileZilla – porniți serverul pe portul 5000.

   b. [25p] Creați o regulă de firewall care să permită traficul FTP din rețeaua internă către WAN1.

   c. [30p] Încercați să vă conectați la serverul colegului pe portul 5000. Funcționează?

   d. [40p] Folosind session-helpers, modificați portul pe care ascultă de obicei FTP în 5000.

   e. [45p] Încercați din nou să vă conectați la serverul colegului pe portul 5000. Funcționează?

3. În cadrul acestui task, studenții vor învăța cum să filtreze anumite aplicații.

   a. [50p] Logați-vă pe facebook, cu mailul test.mssr@gmail.com și parola testing_mssr.

   b. [55p] Creați o listă de application control care să oprească aplicațiile Facebook.

   c. [60p] Aplicați această listă regulii de firewall către Internet. Verificați dacă funcționează o aplicație de Facebook.

   d. [70p] Editați lista și adăugați o regulă care să blocheze și chat-ul de facebook – realizați această operațiune din editarea politicii de firewall. Verificare: pop-out la lista de chat și verificați dacă sunt listate contactele de facebook.

4. Traffic Shaping

   a. [75p] Descărcați fisierul de la acest link. Apreciați cât de repede este acesta descărcat.

   b. [85p] Creați un shared traffic shaper și setați prioritatea medie și bandwidth 50.

   c. Verificați rata de transfer.

5. Application Control Shaper
    a. [90p] Creați o listă de control a aplicațiilor din categoria transferului de fișiere și de tipul Rapidshare care să permită transferurile RapidShare.
    b. Traficul nu trebuie să depășească 100KB, iar banda garantată este de 75KB.
    c. [95p] Aplicați această listă politicii de firewall curente și eliminați toate celelalte restricții aplicate.
    d. [100p]Verificați folosind acest link, dar și log-urile create.
6. Restaurați configurația inițială a echipamentului Fortinet, folosind configurația corespunzătoare din arhivă.