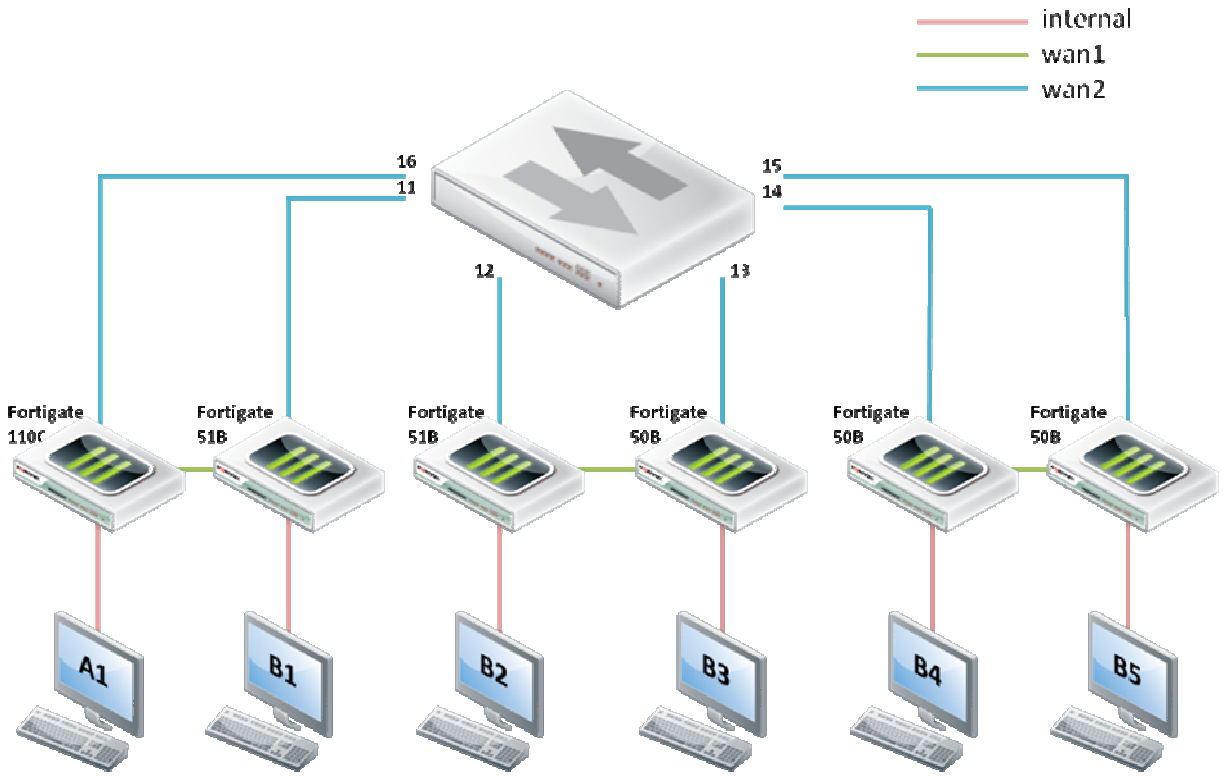
MSSR Fortinet Lab 2 – Politici de firewall

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 accesul prin ssh la echipamentul vostru a stației vecine, pe interfața WAN1. Atenție, fiind particularizări ale politicilor de firewall, acestea vor fi configurate din tab-ul Firewall.

    a. Adăugați o adresă IP din subnet-ul 10.10.10.0/24 pe interfața WAN1.

    b. [20p] Creați o politică de firewall care să permită orice tip de trafic ce vine din rețeaua internă către interfața de WAN1. Accesul va fi translatat.

    c. [25p] Creați un nou grup de servicii, denumit **acces_distanta,** care să permită numai accesul ssh și telnet.

    d. [30p] Modificați politica de firewall creată anterior și adăugați particularizarea.

    e. [40p] Creați un nou administrator normal, denumit **admin_forty**, cu profil super_admin, care va fi folosit de către stația învecinată pentru accesul remote. Verificați că și colegul de link are creat un nou administrator, și logați-vă, de pe stația voastră pe fortigate-ul său prin ssh. Verificați că ping-ul nu funcționează.

3. În cadrul acestui task, studenții vor învăța cum să particularizeze politicile de firewall. La sfârșit, politica de firewall va permite traficul web și ICMP numai a subnet-ului intern, doar în zilele de lucru (de luni până vineri), și numai în intervalul orar 8:00-22:00. Atenție, fiind particularizări ale politicilor de firewall, cerințele următoare vor fi configurate din tab-ul Firewall.

    a. [45p] Creați o adresă denumită **retele_interne,** care să cuprindă subnet-ul de rețele interne.

    b. [50p] Creați un nou grup de servicii, denumit **web,** care să cuprindă numai traficul de tip HTTP, HTTPS, DNS și Ping.

    c. [55p] Creați un nou orar periodic denumit **orar_lucru**, care să cuprindă zilele de lucru (luni-vineri), și intervalul orar 8:00-22:00.

d. [65p] Modificați politica de firewall existentă din intern către Internet pentru a cuprinde cele 3 particularizări. Verificați că doar traficul de tip web funcționează.

4. Politici cu autentificare

   a. [70p] Creați un utilizator local, denumit cu prenumele vostru, și parola tot prenumele vostru.

   b. [75p] Creați un grup de utilizatori, denumit **autentif_firewall**, și adăugați utilizatorul nou creat în acest grup

   c. [90p] Modificați politica de firewall internal->wan2, activând Identity Based Policy. Grupul folosit va fi cel creat la punctul anterior, iar serviciile accesibile vor fi identificate de către grupul web, iar pagina de redirectare va fi una la alegere. Verificați din browser, accesând o pagină web.

   d. [100p] Modificați cele două mesaje de disclaimer, atat *Disclaimer page*, cât și *Declined disclaimer page*. (*Hint:* e o configurare de sistem). Înainte de realizarea acestui subpunct, chemați asistentul pentru validare. Pentru testarea acestei cerințe, trebuie să vă delogați utilizatorul (*Hint:* user>monitor), după care deschideți o nouă pagină web.

5. Restaurați configurația inițială a echipamentului Fortinet, folosind configurația corespunzătoare din arhivă.