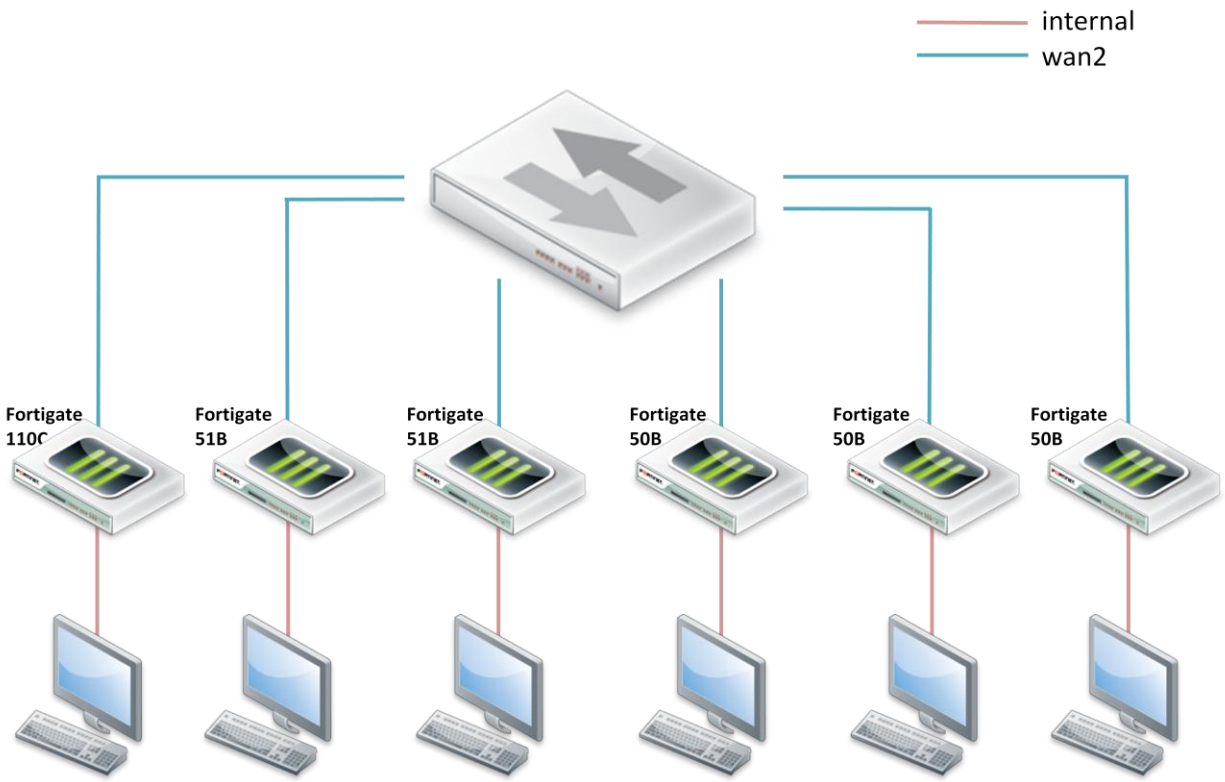
MSSR Fortinet Lab 11 - UTM

1 Topologie



2 Teorie

Unified Thread Management: Filtrare web, Antivirus și DLP.

3 Cerințe

1. [20p] În cadrul acestui task, studenții vor configura echipamentul Fortinet pentru a permite accesul la Internet stației de lucru.

    a. Descărcați arhiva de pe curs.cs.pub.ro, după care conectați stația existentă 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.

b. Verificați că interfața WAN2 își va lua configurațiile și default gateway prin DHCP.

c. Configurați o rută statică default, pentru accesul la Internet prin WAN2.

d. Creați o politică de firewall care să permită accesul intern către Internet. Acest tip de acces va fi NAT-uit.

2. În cadrul acestui task, veți exersa mecanisme de Web Filtering, pentru a permite accesul la anumite URL-uri, precum și blocarea acestora în funcție de conținut.

   a. [30p] Creați un filtru URL pentru blocarea oricărui URL:

      i. Creați un filtru URL, denumit **lista_URL**. Creați o nouă intrare, de tip Regex, care să blocheze orice URL, astfel - introduceți la URL: ^.*$. **Hint:** Pentru mai multe referințe pentru expresii regulate, click [http://regexlib.com/CheatSheet.aspx].

      ii. Atașați acest filtru unui nou profil, denumit **filtru_URL**. Activați HTTP, HTTPS și Logging pentru filtrul URL. **Hint:** UTM>Web Filter>Profile

      iii. Atașați profilul creat politicii de firewall existente. **Hint:** La activarea filtrării web, trebuie definită și o listă Protocol Options – folosiți-o pe cea implicită. După aplicarea profilului, verificați.

   b. [35p] Modificați mesajul de disclaimer default într-unul la alegere. **Hint:** System>Config>Replacement Message>HTTP

   c. [40p] Creați o nouă intrare în filtrul URL, pentru a permite accesul la www.fortinet.com. **Hint:** Pentru a avea prioritate, această intrare va trebui să fie mutată înaintea intrării deja create. Verificați că funcționează și alegeți 2 cuvinte la alegere, precum *security* și *fortiguard.*

   d. [50p] Filtrarea conținutului

      i. Creați un filtru de conținut web denumit **filtru_continut** și adăugați o intrare care să blocheze cuvântul *security*. Intrați pe www.fortinet.com și verificați dacă funcționează. **Hint:** UTM>Web Filter>Web Content Filter, iar pentru activarea filtrării de conținut, trebuie selectată în profilul de filtru web deja folosit, precum și opțiunile HTTP și Logging. Verificați din nou. Această intrare filtrează orice URL conține exact cuvântul *security*.

      ii. Dezactivați intrarea de la punctul anterior și permiteți filtrarea cuvântului *fortiguard*, indiferent de combinația de litere mici/majuscule. **Hint:** Cuvântul trebuie trecut sub forma */fortiguard/i* și este de tipul Regular Expression. Verificați.

   e. [55p] Verificați log-urile create. **Hint:** Log&Report>Log Access

3. Dezactivați filtrul URL. În cadrul acestui task, veți exersa mecanisme de Antivirus.

    a. [60p] Creați un filtru pentru fișierele *.com și *.exe, din meniul Antivirus>File Filter, selectându-le din regula deja existentă, *builtin-patterns.*

    b. [65p] Pentru scanarea după tipuri de grayware malițios, selectați această opțiune din meniul Antivirus>Virus Database.

    c. [70p] Creați un profil de antivirus, denumit **block_com_exe**, pentru care activați toate protocoalele din dreptul Virus Scan și File Filter, precum și opțiunea de Logging.

    d. [75p] Aplicați acest profil regulii existente de firewall.

    e. [80p] Verificați de pe acest site[http://eicar.org/anti_virus_test_file.htm], încercând să descărcați fișierul eicar.com. Analizați și logurile din meniul Log&Report>Log Access>Antivirus.

4. Dezactivați filtrul Antivirus. În cadrul acestui task, veți exersa mecanisme de Data Leak Prevention, pentru a filtra transmiterile datelor sensibile.

    a. [90p] Blocați transferul prin HTTP al fișierelor criptate

        i. Creați o regulă DLP denumită **fis_criptat**, pentru toate fișierele criptate ce vor fi manipulate prin orice metodă HTTP.

        ii. Creați un senzor DLP denumit **block_fis_criptat**, care să blocheze orice trafic conform regulii DLP creată. Activați și Logging-ul.

        iii. Editați politica de firewall pentru a include senzorul creat.

        iv. Verificați, descărcând fișierul de aici [http://campus.training.fortinet.com/mod/tab/view.php?id=3126].

    b. [100p] [Blocați transferul prin HTTP ce conține numere de Visa sau Mastercard.

        i. Modificați regula DLP denumită *HTTP-Visa-Mastercar*, care identifică în conținut numerele de Visa/Mastercard. Activați metoda HTTP GET, și opțiunea de scanare a conținutului arhivelor.

        ii. Creați un senzor DLP denumit **date_sensibile**, care să blocheze traficul identificat de către regula de la punctul anterior, și activați logging-ul.

        iii. Editați politica de firewall pentru a dezactiva senzorul de la punctul a și pentru a-l include pe cel creat.

        iv. Verificați de aici.

c. [110p] Blocați fișierele mp3 supradimensionate.

   i. Creați o nouă regulă DLP denumită **fisiere_mari**, pentru protocolul HTTP, activând toate metodele HTTP. Regula se aplică pentru Transfer Size >= 1000KB.

   ii. Creați un filtru Antivirus pentru fișierele mp3, denumit **no_mp3**.

   iii. Creați o nouă regulă DLP, denumită **regula_mp3,** pentru protocolul HTTP, cu toate metodele HTTP selectate, și care se aplică tipului de fișiere **no_mp3**.

   iv. Creați un compus DLP denumit **fis_mari_mp3**, pentru protocolul HTTP, cu toate metodele HTTP selectate, ce conține regulile **fisiere_mari** și **regula_mp3**. **Hint:** UTM>DLP>Compound.

   v. Editați senzorul **date_sensibile** pentru a bloca regula compusă creată.

   vi. Verificați regula creată, descărcând fișierul.

d. [110p] Verificați log-urile create. **Hint:** Log&Report>Log Access

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