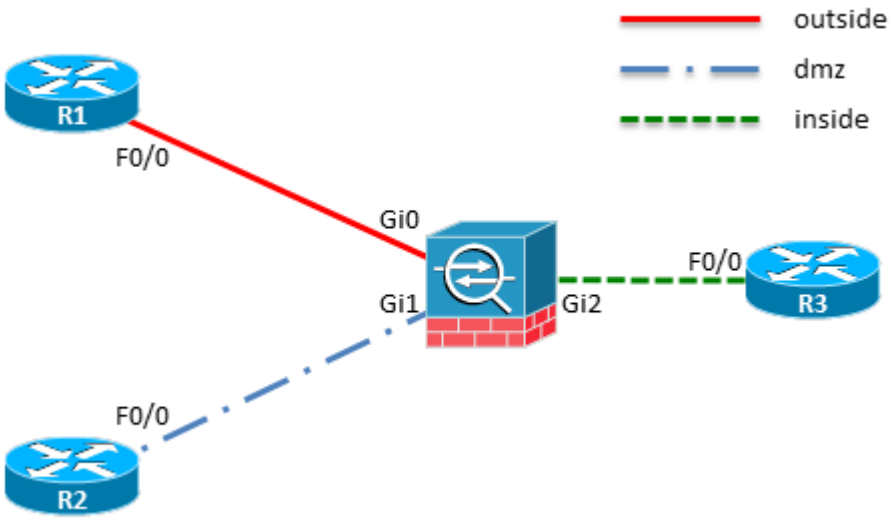
Examen practic - ASA

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 „cisco.com” și „ocw.cs.pub.ro”.
- Singura documentație pe care o puteți folosi o reprezintă slide-urile de curs.

3 Cerințe

1. [5p] Conectare la echipamente și verificarea configurațiilor deja realizate.
    a. [2p] Verificați/Configurați următoarele adrese IP:

Router	Interfață	Adresă IP
R1	F0/0	141.85.99.100/24
R1	Loopback0	1.1.1.1/32
R2	F0/0	10.10.10.100/24
R2	Loopback0	2.2.2.2/32
R3	F0/0	192.168.1.100/24
R3	Loopback	3.3.3.3/32

    b. [3p] Configurați adresarea IP pe interfețele ASA din același spațiu de adrese cu ruterele conectate, folosind „.1” în ultimul octet. (Nu este necesară pornirea interfețelor).

2. [15p] Configurări de bază pentru echipamentul ASA.
    a. [3p] Configurați hostname-ul ASA-ului folosind prenumele vostru. Porniți interfețele folosite. Configurați parola „sred” pentru protejarea modului privilegiat.
    b. [3p] Configurați interfețele ASA pentru a reflecta zonele de securitate din topologie, unde ordinea pentru nivelul de securitate este
        i. zona „outside” < zona „DMZ” < zona „inside”
    c. [3p] Configurați un utilizator nou. Folosiți numele de utilizator „admin” și parola „sredadmin”.
    d. [3p] Configurați ASA pentru a putea accesa folosind comanda „ping” din R3 în R2.
    e. [3p] Configurați ASA pentru a putea realiza conexiuni HTTP din „outside” în „DMZ”. Testați rulând un server HTTP pe ruterul din DMZ.

3. [15p] Configurări avansate de modificare a traficului.
    a. [3p] Realizați configurațiile necesare pentru a putea iniția conexiuni de telnet de pe R3, pe oricare din interfețele de loopback ale ruterelor R1 și R2.
    b. [3p] Configurați rețeaua astfel încât tot traficul din rețeaua 192.168.1.0/24, zona „inside”, către zona „outside” să fie translatat în adresa de pe interfață de a echipamentului ASA.

c. [3p] Realizați configurările necesare astfel încât traficul din rețeaua 10.10.10.0/24, din zona „DMZ”, către „outside” să fie translatat în pool-ul 89.97.65.0/24.

d. [3p] Realizați configurările necesare astfel încât traficul de pe loopbackul lui R2 destinat loopbackului lui R1 să fie translatat în adresa 89.97.66.1/32. Traficul de pe loopbackul lui R2 către orice altă rețea destinație, în afară de loopbackul lui R1, să nu fie translatat.

e. [3p] Configurați rețeaua astfel încât să aveți în continuare conectivitate (ping, telnet, HTTP port 80) între inside (192.168.1.0/24) și DMZ după efectuarea exercițiilor 3b, 3c și 3d.

4. [20p] Criptarea traficului între ASA și R1. Definiți un tunel IPSec pe ASA știind că peer-ul său este ruterul R1, care a fost deja configurat cu politicile de mai jos. Configurați tunelul ținând cont de reflectarea configurațiilor de pe R1. Atenție: informațiile de mai jos sunt configurațiile ce au fost deja realizate pe R1.

   a. [4p] Configurați pe ASA politica de ISAKMP cu următorii parametrii:

      i. Autentificare PSK cu cheia „sred123”

      ii. Criptare 3des

      iii. Hashing SHA

      iv. DF group 2

   b. [4p] Traficul interesant a fost definit pe R1 ca fiind traficul TCP cu sursa 1.1.1.1/32 și destinația 3.3.3.3/32.

   c. [4p] Configurați politica de IPSec pentru a folosi criptare de tip „esp-aes”, autentificare de tip „esp-sha-hmac” și modul de tip tunel.

   d. [8p] Verificați criptarea corectă a traficului.