UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

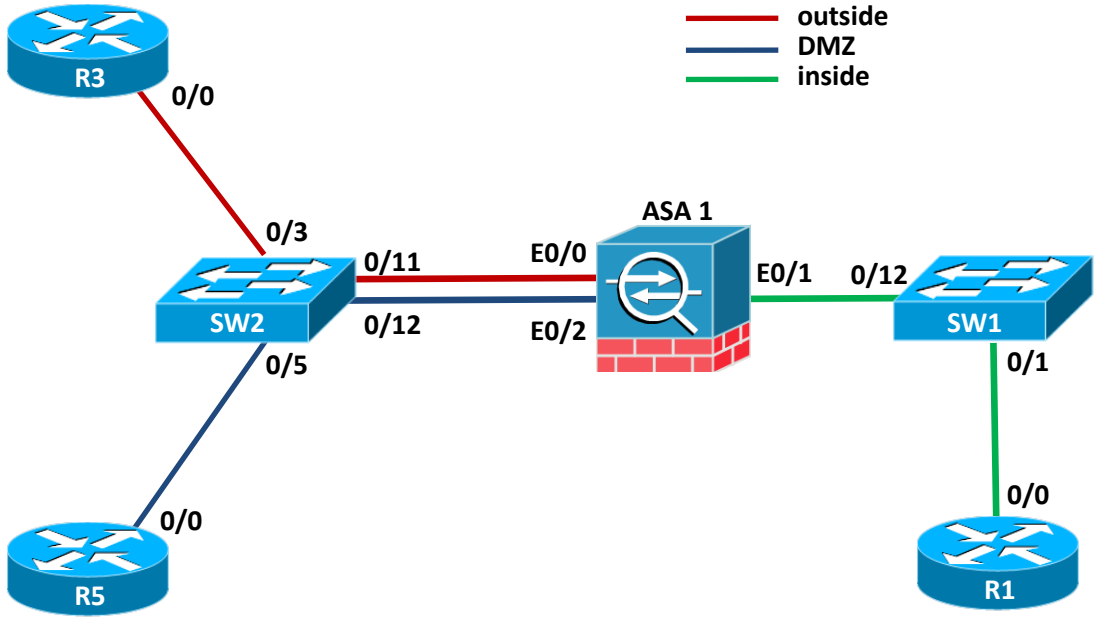
Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

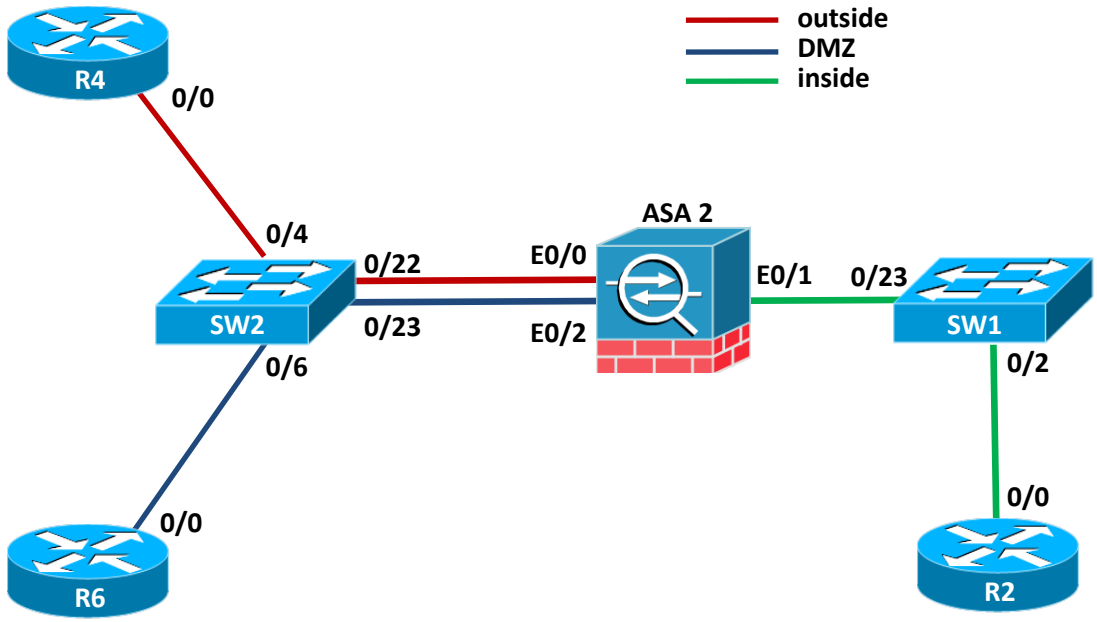
Securizarea rețelelor folosind sisteme dedicate

25. Soluții de remote-access VPN

SRSD 25 – Soluții de remote-access VPN

1 Topologie





2 Obiective

În acest laborator studenții vor învăța să configureze un tunel Site-to-Site IPSec între două dispozitive ASA. Pentru a putea reuși configurația laboratorului, studenții trebuie să lucreze în echipă și să își sincronizeze configurațiile pentru a negociat tunelul.

La finalul laboratorului, studenții vor avea următoarele competențe pe dispozitivele Cisco ASA:

- Activarea ISAKMP pe interfața de ieșire ASA
- Configurarea unei politici de ISAKMP
- Configurarea unui tunel group și a unei chei de autentificare pentru IKE Phase 1
- Definirea unei liste de acces pentru a defini traficul interesant
- Definirea unui transform set pentru IKE Phase 2
- Configurarea unui crypto-map pentru a defini peer-ul remote și a atașa transform-setul
- Verificarea configurației realizate

3 Taskuri

1. În cadrul acestui task studenții vor învăța să configureze un VPN IPSec Site-to-Site între două dispozitive ASA. La configurațiile ce urmează va trebui să comunicați cu colegul vostru pentru a **sincroniza** parametrii IPSec și a avea un tunel funcțional.
    a. Activați ISAKMP pe interfața de ieșire a ASA
    b. Definiți o politică ISAKMP cu următorii parametrii:
        i. Criptare 3DES
        ii. Hashing sha
        iii. Autentificare PSK
        iv. Diffie-Hellman group 5
        v. Lifetime de 86400 secunde
    c. Definiți un tunnel-group de tip site-to-site folosind IP-ul colegului vostru de pe interfața de outside a ASA ca nume al tunnel-group.
    d. Definiți parola PSK cisco123 ca atribut al tunnel-group-ului creat anterior.

e. Definiți un ACL pentru identificarea traficului interesant ca fiind trafic TCP. Rețeaua sursă trebuie să fie rețeaua din care face parte ruterul vostru din zona inside în timp ce rețeaua destinație trebuie să fie cea din care face parte ruterul colegului din zona inside.

f. Definiți un transform set care să folosească ESP-3DES pentru criptare și SHA-HMAC pentru autentificare.

g. Definiți un crypto-map care să specifice

    i. Adresa de peer -> adresa IP a colegului vostru de pe interfața outside a ASA

    ii. ACL-ul ce definește traficul interesant

    iii. Transform-setul configurat anterior

h. Aplicați crypto-map-ul pe interfața de outside

i. Testați tunelul IPSec generând trafic interesant de la R1 la R2. Verificați că s-au generat SA-urile ISAKMP și IPSec și numărul de pachete criptate.