UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale 2007-2013

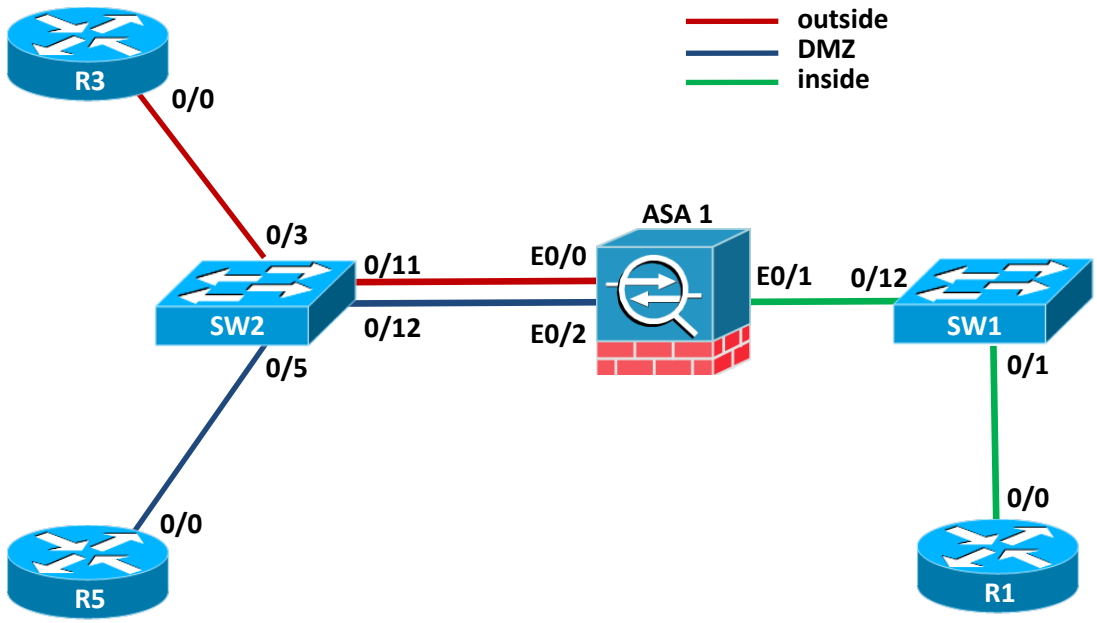
Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

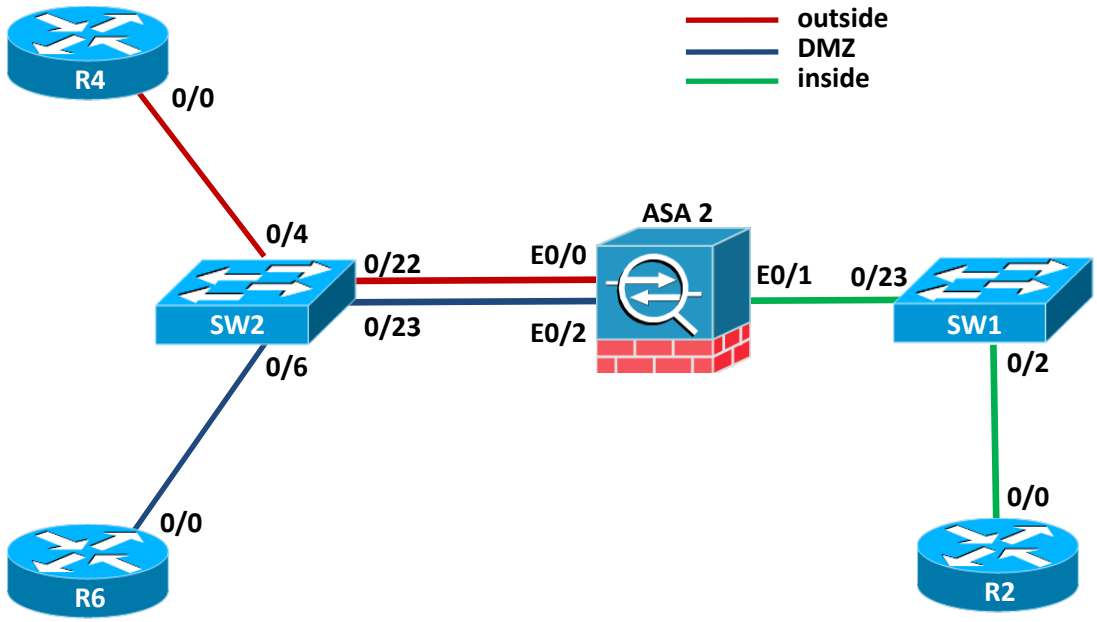
Securizarea rețelelor folosind sisteme dedicate

31. Tehnici de optimizare a comunicatiilor WAN

SRSD 31 – Tehnici de optimizare a comunicatiilor WAN

1 Topologie





2 Obiective

În acest laborator studenții vor învăța să configureze un tunel IPSec Remote-Access VPN folosind Easy VPN Server pe ASA OS alături de clientul Easy VPN din Cisco IOS configurat în modul Network Extension Mode.

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 atributelor Remote-Access
- Definirea unui tunnel-group de tip remote-access
- Configurarea unui pre-shared key în cadrul atributelor de tunel
- Configurarea parametrilor primiți de client în Mode-Config
- Configurarea autentificării locale și a conturilor de VPN în XAUTH
- Definirea transform-setului pentru generarea SA-urilor IPSec
- Definirea crypto-map-ului dinamic
- Configurarea unui crypto-map static care să identifice crypto-mapul dinamic
- Aplicarea crypto-mapului static pe interfață pentru a putea iniția tunelul IPSec
- Configurarea clientului Easy VPN în IOS în modul Network Extension Mode

3 Taskuri

1. În cadrul acestui task studenții vor învăța să configureze parametrii ISAKMP necesari unui tunel IPSec Remote-Access
    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.