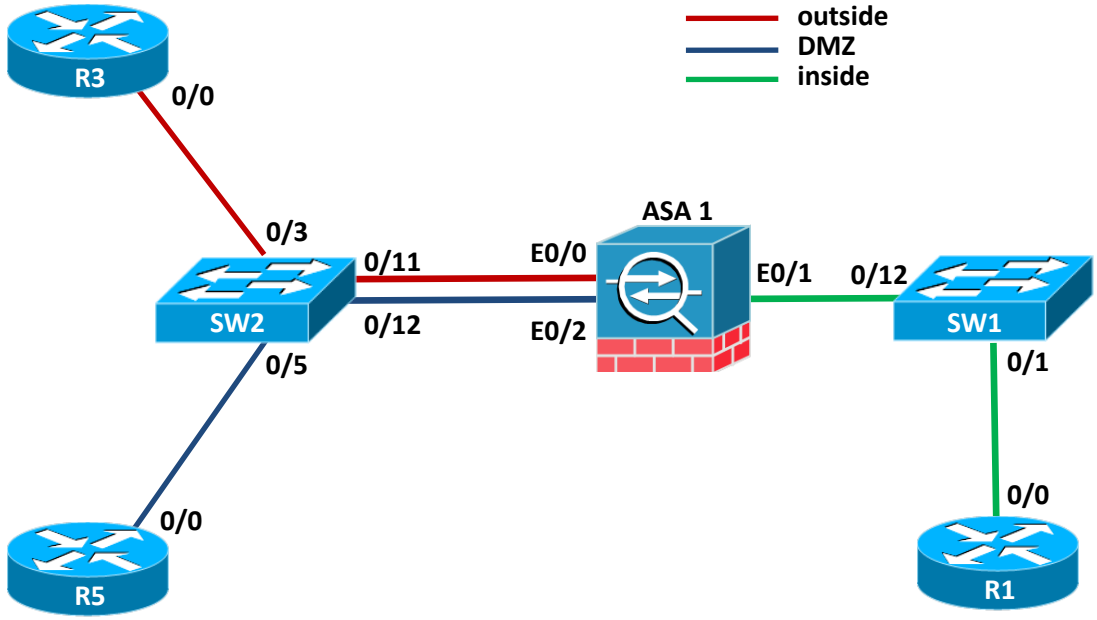
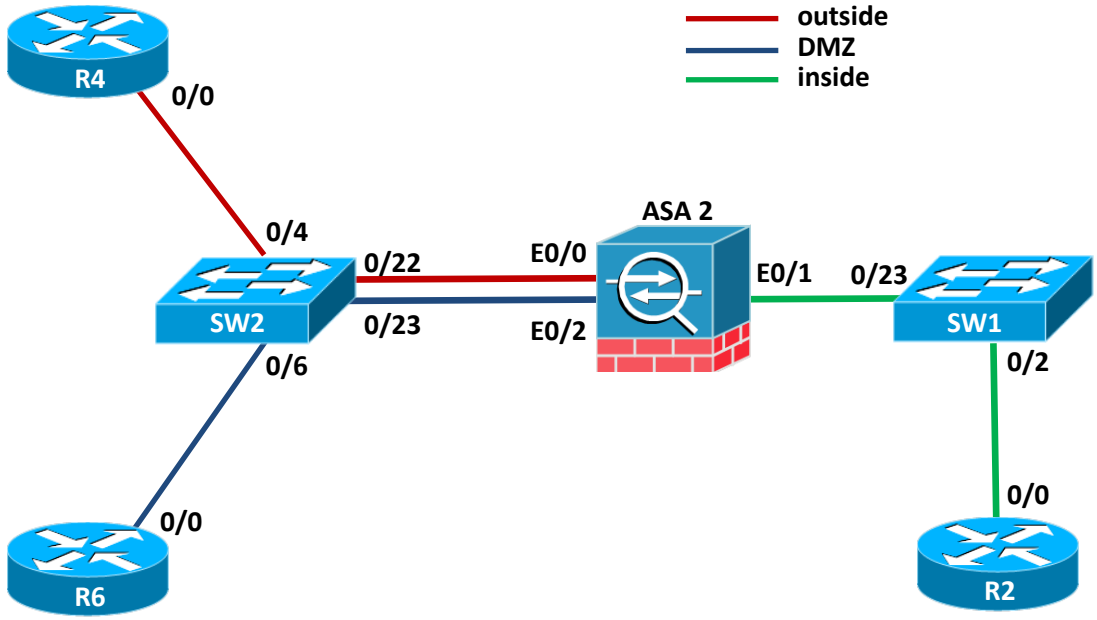
MSSR Cisco Lab 8 – IPSec Remote-Access

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 cum să realizeze configurațiile de bază pe un echipament ASA

    a. Descărcați de pe cs.curs.pub.ro arhiva acces_echipamente_cisco.zip

    b. Dezarvați cele 3 fișiere .reg din interiorul arhivei și întrebați asistentul vostru cum să procedați în continuare

    c. Conectați-vă la echipamentele din topologia de mai sus funcție de distribuția realizată de asistent

2. În cadrul acestui task studenții vor recapitula configurarea parametrilor de bază pe ASA OS și Cisco IOS pentru a asigura conectivitatea L3 necesară tunelului IPSec.

    a. [2p]Configurați hostname-ul ASA-ului folosind prenumele vostru.

    b. [25p]Configurați ASA cu următorii parametrii:

- Configurați interfața E0/1 ca **inside** și E0/0 ca **outside**
- Adresă IP E0/1: 192.168.1.1/24
- Adresă IP E0/0: 141.85.99.1/24

c. Configurați ruterul din zona **inside** cu următorii parametrii:
- Adresă IP: 192.168.1.100/24
- Rută default către ASA cu next-hop 192.168.1.1

d. Configurați ruterul din zona **outside** cu următorii parametrii:
- Adresă IP: 141.85.99.100/24
- Rută default către ASA cu next-hop 141.85.99.1

e. Configurati pe ruterul din zona outside o interfata de loopback cu adresa IP 5.5.5.5/32.

f. Definiti o ruta statica pe ASA pentru a putea ajunge la reteaua 5.5.5.5

g. Verificati conectivitatea intre loopback si ASA si intre ruterul din interior si ruterul din exterior inainte de a incepe configuratiile de VPN

3. În cadrul acestui task studenții vor învăța să configureze parametrii 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 remote-access

d. Definiți parola PSK cisco123 ca atribut al tunnel-group-ului creat anterior.

e. Definiți ACL-ul 102 pentru identificarea traficului interesant ca fiind trafic TCP intre reteaua de loopback a ruterului din zona outside si ruterul din zona inside.

f. Definti un group-policy numit MSSR de tip internal si definiti urmatoarele configuratii
    i. un server de DNS cu valoarea 4.2.2.2
    ii. activati optiunea “nem enable” pentru a putea avea un client remote in acest mod
    iii. activati posibilitatea de a stoca parole intern in cadrul acestui grup prin parametrul “password-storage”
g. Definiti utilizatorul cisco cu parola cisco123
h. Definiti urmatoarele atribute pentru utilizatorul cisco
    i. vpn-group-policy = MSSR
    ii. vpn-filter-value = 102, unde 102 este lista de acces definita anterior.
    iii. vpn-framed-ip-address = 10.10.10.100
i. Definiți un transform set care să folosească ESP-3DES pentru criptare și SHA-HMAC pentru autentificare.
j. Configurati un dynamic-map care sa referentieze transform-setul configurat anterior
k. Configurati un crypto map care sa referentieze dynamic-mapul anterior
l. Aplicati crypto-mapul pe interfata de iesire a ASA

4. În cadrul acestui task studenții vor învăța să configureze clientul Easy VPN in modul NEM in Cisco IOS
    a. Activati clientul de VPN remote-access cu urmatorii parametrii
        i. configurati modul de conectare pentru a fi automat
        ii. configurati grupul de VPN cu acelasi nume ca pe ASA si aceeasi cheie partajata
        iii. configurati modul clientului la network-extension
        iv. configurati peer-ul la adresa IP de pe interfata de outside a ASA
        v. configurati numele de utilizator cisco cu parola cisco123
    b. Specificati Fa0/0 ca interfata de outside pentru clientul Easy VPN
    c. Specificati Lo0 ca interfata de inside pentru clientul Easy VPN
    d. Conectati-va folosit telnet de pe loopbackul ruterului din outside, pe ruterul din inside.