



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI



Instrumente Structurale
2007-2013

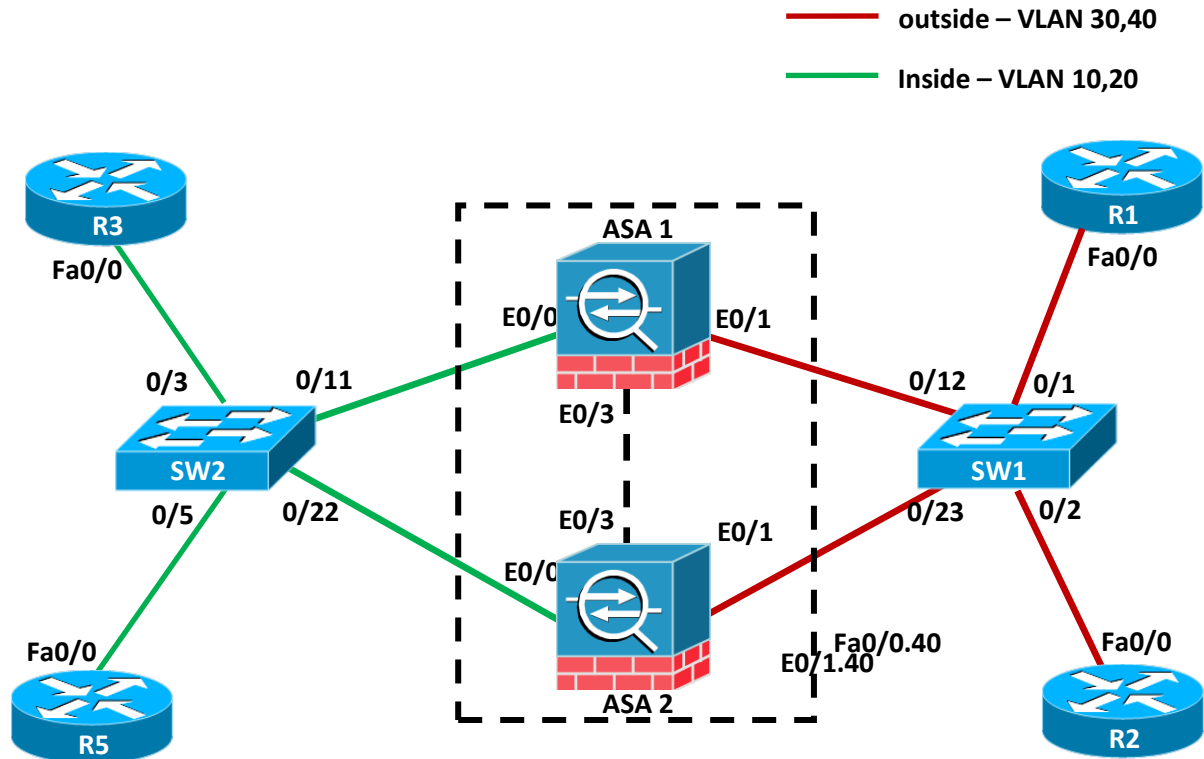


Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Securizarea rețelelor folosind sisteme dedicate

35. Soluții de UTM: Antivirus, Antispam, Antispyware, DLP

1 Topologie



2 Obiective

În acest laborator studenții vor învăța să configureze funcționalitatea de High-Availability ASA pentru a oferi un grad ridicat de redundanță securității unei rețele interne.

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

- Configurarea ASA pentru un scenariu de bază în high-availability
- Configurarea ASA în modul primary sau secondary pentru a influența alegerea unității active sau standby
- Configurarea ASA pentru LAN-Based failover
- Configurarea funcționalității de stateful failover peste o legătură dedicată
- Configurarea interfețelor monitorizate între cele 2 echipamente în HA
- Testarea diferitelor scenarii de HA

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 configura switchurile din rețea pentru a pregăti infrastructura de L2 pentru failover.
 - a. Intrați pe toate ruterele din topologie și asigurați-vă că au configurații default.
 - b. [2p]Configurați SW1 astfel încât R1 și ASA1 să fie în același VLAN, dar fără ca acest VLAN să conțină și alte interfețe
 - c. [4p]Configurați SW2 astfel încât R3 și ASA1 să fie în același VLAN, dar fără ca acest VLAN să conțină și alte interfețe
3. În cadrul acestui task studenții vor învăța să configureze unitatea primary ASA.
 - a. Configurați mai întâi ASA1. Dacă nu are configurații implicite, folosiți comanda `clear configure all`.
 - b. [6p]Configurați hostname-ul ASA-ului la valoarea: ASA1
 - c. [8p]În primul scenariu, ASA1 va juca rolul ASA-ului primary și activ. Configurați interfața E0/3 a ASA 1 ca interfață de failover de comandă cu numele „Control”.
 - d. [10p]Folosiți comanda `sh run int e0/3` pentru a inspecta comenzile automat generate pe această interfață. Activați interfața `e0/3`.
 - e. [15p]Realizați următoarele configurații pe interfața E0/0
 - i. Numele inside cu nivelul de securitate 100
 - ii. adresa IP 192.168.1.1/24 pe interfața E0/0 cu adresa de standby 192.168.1.2
 - f. [20p]Realizați următoarele configurații pe interfață E0/1
 - i. Numele outside cu nivelul de securitate 0
 - ii. adresa IP 141.85.99.1/24 pe interfața E0/1 cu adresa de standby 141.85.99.2

- g. [30p]Configurați adresa IP de failover 11.11.11.1 pentru unitatea activă și adresa de failover 11.11.11.2 pentru echipamentul care va fi secundar (standby).
 - h. [35p]Configurați această unitate ca unitate primară de failover.
 - i. [40p]Activați procesul de failover folosind comanda **failover**.
4. În cadrul acestui task studenții vor învăța să configureze unitatea secondary de ASA și să evalueze funcționarea ASA HA.
- a. [45p]Configurați acum ASA2. Dacă nu are configurații implicite, folosiți comanda `clear configure all`.
 - b. [47p]Configurați hostname-ul ASA-ului la valoarea: ASA2
 - c. [50p]Configurați interfața **e0/3** ca interfața de LAN failover. Activați interfața folosind `no shutdown`.
 - d. [55p]Configurați adresa IP 11.11.11.1 ca adresă pentru unitatea activă și adresa de failover 11.11.11.2
 - e. [60p]Configurați această unitate ca unitate secundară de failover.
 - f. [65p]Activați procesul de failover folosind comanda **failover**.
 - g. [67p]Așteptați câteva secunde. Ce observați că s-a întâmplat în rețea? Care este explicația? [Folosiți comanda **show failover state** pentru a verifica statusul de activ sau standby al unui ASA]
 - h. [70p]După ce s-a renegociat unitatea activă, verificați hostname-ul ASA-ului aflat în standby. Ce observați?
 - i. [70p]Dați comanda **sh int ip br** pe fiecare dintre cele 2 ASA. Ce observați?
5. În cadrul acestui task studenții vor învăța să monitorizeze ASA HA.
- a. [72p]Configurați switchurile pentru a include și interfața către ASA2 și către ruterele din partea de jos a topologiei în același VLAN cu cel în care ați introdus inițial ASA1 și ruterele R1 și R3.
 - b. [75p]Configurați adrese IP și rute default pe cele 4 rutere .
 - c. [80p]Configurați inspecția ICMP pe ASA-ul activ. Verificați faptul că s-a replicat configurația pe ASA-ul standby.
 - d. [82p]Configurați parolă de telnet și de enable pe ambele rutere. Salvați configurația pe ASA-ul activ.

- e. [85p] Porniți un ping de 5000 de pachete de la ruterul R3 la R1. În același timp porniți o sesiune de telnet de la R5 la R2 și autentificați-vă.
- f. [90p] În timp ce ping-ul rulează și conexiunea de telnet este activă, rebootați ASA-ul activ. Ce s-a întâmplat cu ping-urile? Dar cu sesiunea de telnet?
- g. [100p] Configurați ASA failover pentru ca sesiunea de telnet să se păstreze în eventualitatea unui failover. Testați rebootând încă o dată ASA-ul activ.