UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

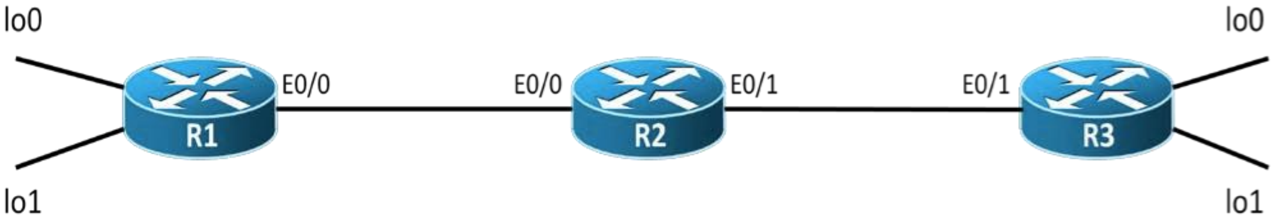
Instrumente Structurale
2007-2013

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

Securizarea Calculatoarelor și a Rețelelor

30. Implementarea VPN-urilor IPSec Site-to-Site

Topology



Device	Interface	IP Address	Subnet Mask
R1	F0/0	192.168.12.1	255.255.255.248
R1	Lo0	10.1.1.1	255.255.255.0
R1	Lo1	11.1.1.1	255.255.255.0
R2	F0/0	192.168.12.2	255.255.255.248
R2	F0/1	192.168.23.2	255.255.255.248
R3	F0/0	192.168.23.3	255.255.255.248
R3	Lo0	10.3.3.3	255.255.255.0
R3	Lo1	11.3.3.3	255.255.255.0

Tasks

1. [2p] Configure the above topology with the IP addresses shown in the IP Addressing table. Configure EIGRP/OSPF in the above topology in order to have end-to-end connectivity.
    a. Do an extended from R1's lo1 interface to R3's lo1 interface.
2. [+5p=7p] Configure so that traffic between R1 Lo0 and R3 Lo0 is encrypted using IPSec.
    a. Configure the following ISAKMP policy on both R1 and R3
        i. authentication: pre-shared keys
        ii. encryption: aes 256
        iii. hashing: sha1
        iv. diffie-hellman group: 2
        v. lifetime: 3600
    b. Configure "srs!@#" as a pre-shared key on both R1 and R3.
    c. Configure the following transform set on both R1 and R3:
        i. Tag (name of the transform set): *TS_SRS*
        ii. Transform set: esp-aes 256 esp-sha-hmac
        iii. Mode: transport
    d. Construct an access-list that will match the traffic that you want to encrypt. The access-list will have to define both the source and the destination of the traffic. An access-list must be defined on both R1 and R3. **Watch out for the fact that the 2 ACLs must mirror each other.**
    e. Create a crypto-map called ***TUNNEL_MAP*** on both R1 and R3.
        i. The crypto map must match the ACL that you used to define interesting traffic.
        ii. The crypto map must set the remote peer for the tunnel. The remote peer is going to be the IP address of the outgoing Ethernet interface of each router.
        iii. The crypto map must set the transform set to "TS_SRS"
    f. Apply the crypto map on interface F0/0 of R1 and F0/1 of R3.
    g. Verifying that the traffic is encrypted.
        i. Use the "capture R2 F0/0 tunnel.cap" command in the dynagen console to start a capture on R2's F0/0 interface
        ii. Generate traffic between loopback interfaces.
        iii. Stop the capture using the "no capture R2 F0/0" command in the dynagen console.
        iv. Open the tunnel.cap file with Wireshark.