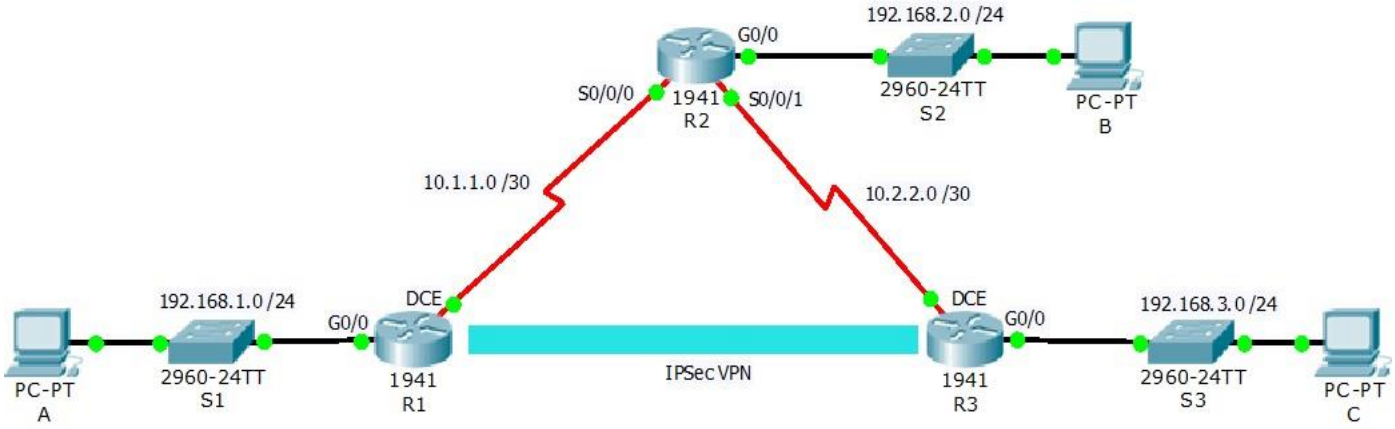

1. Uređaji u šemi i povezivanje

- Switch: 2960
- Router: 1941, dodati moduo *HWIC-2T* u desni slot

Povezivanje

- Ruter – Ruter: Serijska veza
- Ruter – Svič: Straight-Through, koristiti Gigabit Ethernet

2. Standardna podešavanja (IP adresiranje)

Ruteri:

- Standardno podešavanje serijskog interfejsa: clock rate na DCE strani, dodeliti IP adresu, no shutdown
- Standardno podešavanje Ethernet interfejsa: dodeliti IP adresu, no shutdown
- Kopirati running konfiguraciju u startup konfiguraciju sa **`copy run start`**

Računari: dodeliti IP adrese i definisati *Default Gateway*

3. Aktivacija *security* modula

Da proverite da li je Security Technology-package licenca aktivirana, unesite komandu **`show version`**:

```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524ZE75


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

Aktivacija securityk9 modula:

```
R1(config)# license boot module c1900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

Ponoviti isto na ruteru R3.

*** PAŽNJA! module c1900 je uzeto iz rezultata komande show version. Ako ste koristili drugi model rutera, ovaj modul može biti drugačiji.
*** Posle prve komande, prihvatiti licencu sa YES

Detaljnije o licencama vezanim za bezbednost, šta je uključeno u standardni (besplatni) Cisco paket, a šta donose specijalne licence:
http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78-556151.html

4. Konfiguracija IPsec parametara

R1

Treba napraviti ACL koja će identifikovati saobraćaj koji ide iz 192.168.1.0 (R1) prema 192.168.3.0 (R3) kako bi se prepoznali paketi koji treba da idu preko IPSec VPN-a. Ti paketi će biti kriptovani. Sva druga komunikacija neće.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

ISAKMP 1. faza:

```
R1(config)# crypto isakmp policy 10
```

```
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.1
```

U prvoj, "setup" fazi, uređaji se dogovaraju kako da daljnje informacije razmenjuju bezbedno – kreira se SA za sam ISAKMP koji se onda koristi za sigurniju razmenu parametara u drugoj fazi.

ISAKMP 2. faza:

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.1
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Povezati kripto-mapu sa izlaznim interfejsom:

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

R3 treba konfigurisati analogno ruteru R1:

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.1

R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit

R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

5. Rutiranje

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

R2(config)#ip route 192.168.1.0 255.255.255.0 s0/0/0
R2(config)#ip route 192.168.3.0 255.255.255.0 s0/0/1
```

6. Verifikacija

1. R1# show crypto ipsec sa

   Obratiti pažnju na redove:
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

2. Pingovati A-C

3. R1# show crypto ipsec sa

```
R3(config)#do sh cry ipsec sa

interface: Serial0/0/1
    Crypto map tag: VPN-MAP, local addr 10.2.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.2.2.1, remote crypto endpt.:10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x68E14EF2(1759596274)

     inbound esp sas:
      spi: 0x6DB91A19(1840847385)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3592)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x68E14EF2(1759596274)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3592)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

R3(config)#
```