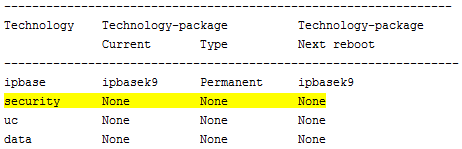
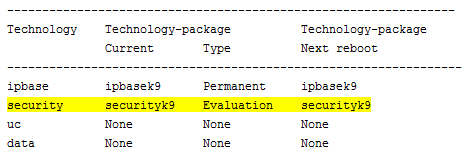
**Part 1:     Security szerepek engedélyezése.**

**Step 1:     Aktiválja a securityk9 modult R1-re és R3-ra.**

Ellenőrzéshez használja a **show version** parancsot.



R1(config)# license boot module c2900 technology-package securityk9  
R1(config)# end  
R1# wr  
R1# reload  
  


**Part 2:**     **IPsec Paraméterek konfigurálása azon R1-en.**

**Step 1:    Csatlakozás tesztelése.**  
Pingelje meg PC-A-ról a PC-C-t.  
  
**Step 2:     Részforgalom azonosítása az R1-en.**

Állítsa be az ACL 110-et, az R1-es LAN-ból az R3 LAN-ba irányuló forgalom engedélyezésére. A LAN-okból származó többi forgalom nem lesz titkosítva. Ne feledje, hogy az implicit tagadás miatt nincs szükség a deny any hozzáadására.  
  
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0

0.0.0.255

**Step 3:     Az ISAKMP 1. fázis tulajdonságainak konfigurálása R1-re.**

Konfigurálja az ISAKMP policy 10 tulajdonságát az R1-en. Az előre megosztott kulcs: **cisco**. Lásd az ISAKMP 1. fázis táblázatát a konfigurálandó paraméterekhez. Az alapértelmezett értékeket nem kell konfigurálni, ezért csak a titkosítást, a kulcscsere módot és a DH módot kell.

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 10.2.2.2

**Step 4:** **Az ISAKMP 2. fázis tulajdonságainak konfigurálása R1-re.**

Hozzon létre egy VPN-SET nevű transform-set-et az esp-3des és az esp-sha-hmac használatához. Ezután hozza létre a VPN-MAP kriptográfiai térképet, amely összekapcsolja a 2. fázis összes paraméterét. Használja a 10-es sorozatszámot és azonosítsa azt ipsec-isakmp-ként.  
  
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 10.2.2.2  
R1(config-crypto-map)# set transform-set VPN-SET  
R1(config-crypto-map)# match address 110  
R1(config-crypto-map)# exit

**Step 5:**    **Konfigurálja a kriptográfiai térképet a kimenő interfészen.**  
Végül kösse össze a VPN-MAP kriptográfiai térképet a kimenő Serial 0/0/0 interfésszel.

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

**Part 3:     Konfigurálja az IPsec paramétereket az R3-on.**

**Step 1:     Állítsa be az R3-at, hogy támogassa a site to site VPN-t az R1-el.**

Most állítsuk be a paramétereket R3-ra. Állítsa be a 110-es ACL-t, amely engedélyezi az R3-as LAN-ról az R1-es hálózatra irányuló forgalmat.  
  
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

**Step 2:    Az ISAKMP 1. fázis tulajdonságainak konfigurálása R3-ra.**  
  
Konfigurálja az ISAKMP policy 10 tulajdonságát az R3-on. Az előre megosztott kulcs: **cisco**.

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 10.1.1.2

**Step 3:   Az ISAKMP 2. fázis tulajdonságainak konfigurálása R3-ra.**

Az R1-hez hasonlóan, létrehozza a VPN-SET transform-set-et az esp-3des és az esp-sha-hmac használatához. Ezután hozza létre a VPN-MAP kriptográfiai térképet, amely összekapcsolja a 2. fázis összes paraméterét. Használja a 10-es sorozatszámot és azonosítsa azt ipsec-isakmp térképként.

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 10.1.1.2  
R3(config-crypto-map)# set transform-set VPN-SET  
R3(config-crypto-map)# match address 110  
R3(config-crypto-map)# exit

**Step 4:    Konfigurálja a kriptográfiai térképet a kimenő interfészen.**  
  
Végül kösse össze a VPN-MAP kriptográfiai térképet a kimenő Serial 0/0/1 interfésszel.  
R3(config)# interface S0/0/1  
R3(config-if)# crypto map VPN-MAP

**Part 4:     IPsec VPN ellenőrzése.**

**Step 1:    Ellenőrizze az alagúton átmenő forgalmat..**  
  
Adja ki a show **crypto ipsec sa** parancsot R1-en. Vegye észre, hogy a beágyazott, titkosított, dekódolt és visszafejtett csomagok száma 0-ra van állítva.  
  
**R1# show crypto ipsec sa**  
  
interface: Serial0/0/0  
    Crypto map tag: VPN-MAP, local addr 10.1.1.2  
  
   protected vrf: (none)  
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)  
   current\_peer 10.2.2.2 port 500  
    PERMIT, flags={origin\_is\_acl,}  
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0  
   #pkts decaps: 0, #pkts decrypt: 0, #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 0, #recv errors 0  
  
     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2  
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0  
     current outbound spi: 0x0(0)  
<output omitted>  
  
**Step 2:     Hozzon létre forgalmat.**  
  
Pingelje meg PC-C-ről a PC-A-t.  
  
**Step 3:     Újra nézze meg az alagúton lévő forgalmat.**  
  
**R1# show crypto ipsec sa**  
  
interface: Serial0/0/0  
    Crypto map tag: VPN-MAP, local addr 10.1.1.2  
  
   protected vrf: (none)  
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)  
   current\_peer 10.2.2.2 port 500  
    PERMIT, flags={origin\_is\_acl,}  
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0  
   #pkts decaps: 3, #pkts decrypt: 3, #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.: 10.1.1.2, remote crypto endpt.:10.2.2.2  
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0  
     current outbound spi: 0x0A496941(172583233)  
<output omitted>