Összefoglaló

Zanzásított verzió

A konkrét IP címek és hálózat címek helyett olyanokat írok mint "local.sub.net" vagy "remote.public.ip". Ahol a két oldal konfigurációja azonos vagy nagyon hasonló, ott csak az egyik oldalt írom ki.

```
; 1. NTP beállítása
/system clock set time-zone-autodetect=yes time-zone-name=Europe/Budapest
/system ntp client set \
    server-dns-name=0.hu.pool.ntp.org,1.hu.pool.ntp.org \
    primary-ntp=[/resolve 2.hu.pool.ntp.org] \
    secondary-ntp=[/resolve 3.hu.pool.ntp.org]

; 2. FQDN beállítása - készíts DNS neveket a router-jeidhez
; ...

; 3. Tanúsítványok generálása és aláírása
; /certificate add name=ca.myserver.hu ... key-usage=digital-signature,....
; /certificate add name=office.myserver.hu ... key-usage=tls-server
; /certificate add name=branch01.myserver.hu ... key-usage=tls-server
; /certificate sign ca.myserver.hu
; /certificate sign office.myserver.hu ca=ca.myserver.hu
; /certificate sign branch01.myserver.hu ca=ca.myserver.hu

; 4. peer tanúsítványok fölmásolása és importálása
; ...

; 5. IKE phase1 proposal beállítása
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 hash-algorithm=sha256 \
    name="myserver.hu" nat-traversal=no proposal-check=strict



; 5. IKE phase2 proposal beállítása
/ip ipsec proposal
```

```
add auth-algorithms=sha256 enc-algorithms=aes-256-cbc pfs-group=modp2048 \
    name="proposal-myserver.hu" lifetime=30m

; 6. ipsec peer-ek létrehozása

/ip ipsec peer
add exchange-mode=ike2 name="peer-remote" \
    address=remote.public.ip/32 \
    local-address=local.public.ip \
 passive=yes send-initial-contact=yes \
    profile="myserver.hu"

; 7. identity létrehozása

; teljes cert azonosítással
/ip ipsec identity
add auth-method=digital-signature peer=peer-branch01 \
    certificate=office.myserver.hu  my-id=fqdn:office.myserver.hu  \
    match-by=certificate remote-certificate=branch01.myserver.hu remote-
id=fqdn:branch01.myserver.hu

; remote-id azonosítással
/ip ipsec identity
add auth-method=digital-signature peer=peer-office \
    certificate=branch01.myserver.hu  my-id=fqdn:branch01.myserver.hu  \
    match-by=remote-id remote-id=fqdn:office.myserver.hu

; 8. policy létrehozása

/ip ipsec policy
add peer=peer-branch01 proposal=proposal-myserver.hu
 dst-address=remote.subnet/24 src-address=local.subnet/24
    tunnel=yes

; 9. NAT bypass

/ip firewall nat
set [find where action=masquerade] ipsec-policy=out,none

; 10. Prevent package leak
```

```
/ip route
add comment="Prevent package leak RFC1918 class A" distance=1 dst-address=10.0.0.0/8
type=unreachable
add comment="Prevent package leak RFC1918 class B" distance=1 dst-address=172.16.0.0/12
type=unreachable
add comment="Prevent package leak RFC1918 class C" distance=1 dst-address=192.168.0.0/16
type=unreachable

; 11.  Add active route to remote subnet

/interface bridge
add name=ipsec protocol-mode=none
/ip route
add dst-address=remote.subnet/24 gateway=ipsec pref-src=local.lan.ip comment="VPN to branch01"

; 12.  replace host unreachable with network unreachable

/ip firewall filter
add action=reject chain=forward out-interface=ipsec \
reject-with=icmp-network-unreachable \
    comment="Reply with network-unreachable when IPSEC tunnel is down"
    place-before=<???>

; 13.  MTU, TCP MSS Clamping

/ip firewall mangle add action=change-mss chain=forward new-mss=1360 \
    src-address=remote.sub.net/24 protocol=tcp tcp-flags=syn tcp-mss=!0-1360 \
    ipsec-policy=in,ipsec passthrough=yes \
    comment="IKE2:  Clamp TCP MSS from remote.sub.net/24 to ANY"
```

Itt további magyarázat nélkül közlöm az office és branch01 router-ek teljes konfigurációját.

office

```
/interface bridge
add name=bridge-office
add name=ipsec protocol-mode=none
/interface ethernet
```

```
set [ find default-name=ether1 ] name=ether1-internet
/interface list
add name=LAN
add name=WAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 hash-algorithm=sha256 name=myserver.hu proposal-
check=strict
/ip ipsec peer
add exchange-mode=ike2 local-address=100.3.3.10 name=peer-branch01 passive=yes
profile=myserver.hu
/ip ipsec proposal
add auth-algorithms=sha256 enc-algorithms=aes-256-cbc name=proposal-myserver.hu pfs-
group=modp2048
/ip pool
add name=pool-office ranges=172.16.2.100-172.16.2.200
/ip dhcp-server
add address-pool=pool-office disabled=no interface=bridge-office name=dhcp-office
/interface bridge port
add bridge=bridge-office interface=ether2
add bridge=bridge-office interface=ether3
/interface list member
add interface=ether1-internet list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
/ip address
add address=172.16.2.1/24 interface=bridge-office network=172.16.2.0
add address=100.3.3.10/24 interface=ether1-internet network=100.3.3.0
/ip dhcp-server network
add address=172.16.2.0/24 dns-server=172.16.2.1 gateway=172.16.2.1
/ip dns
set allow-remote-requests=yes servers=100.3.3.3
/ip firewall filter
add action=accept chain=input comment="Allow UPD 500,4500 for IKEv2" dst-address=100.3.3.10
dst-port=500,4500 in-interface=ether1-internet protocol=udp
add action=accept chain=input comment="Allow IPSEC/ESP" dst-address=100.3.3.10 in-
interface=ether1-internet protocol=ipsec-esp
```

```
add action=accept chain=input comment="defconf: accept established,related,untracked"
connection-state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-
list=!LAN
add action=accept chain=forward ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept established,related, untracked"
connection-state=established,related,untracked
add action=reject chain=forward comment="Reply with network-unreachable when IPSEC tunnel is
down" out-interface=ipsec reject-with=icmp-network-unreachable
add action=drop chain=forward comment="defconf:  drop all from WAN not DSTNATed" connection-
nat-state=!dstnat connection-state=new in-interface-list=WAN
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
/ip firewall mangle
add action=change-mss chain=forward comment="IKE2: Clamp TCP MSS from 172.16.1.0/24 to ANY"
ipsec-policy=in,ipsec new-mss=1360 passthrough=yes protocol=tcp src-address=172.16.1.0/24 \
    tcp-flags=syn tcp-mss=!0-1360
/ip firewall nat
add action=masquerade chain=srcnat ipsec-policy=out,none out-interface=ether1-internet
/ip ipsec identity
add auth-method=digital-signature certificate=office.myserver.hu match-by=certificate my-
id=fqdn:office.myserver.hu peer=peer-branch01 policy-template-group=branch01.myserver.hu \
    remote-certificate=branch01.myserver.hu remote-id=fqdn:branch01.myserver.hu
/ip ipsec policy
add dst-address=172.16.1.0/24 peer=peer-branch01 proposal=proposal-myserver.hu sa-dst-
address=100.2.2.10 sa-src-address=100.3.3.10 src-address=172.16.2.0/24 tunnel=yes
/ip route
add distance=1 gateway=100.3.3.3
add comment="Prevent package leak RFC1918 class A" distance=1 dst-address=10.0.0.0/8
type=unreachable
add comment="Prevent package leak RFC1918 class B" distance=1 dst-address=172.16.0.0/12
type=unreachable
add comment="VPN to branch01" distance=1 dst-address=172.16.1.0/24 gateway=ipsec pref-
src=172.16.2.1
add comment="Prevent package leak RFC1918 class C" distance=1 dst-address=192.168.0.0/16
type=unreachable
/system identity
set name=office.myserver.hu
```

branch01

```
/interface bridge
add name=bridge-branch01
add name=ipsec protocol-mode=none
/interface ethernet
set [ find default-name=ether1 ] name=ether1-internet
/interface list
add name=LAN
add name=WAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 hash-algorithm=sha256 name=myserver.hu proposal-
check=strict
/ip ipsec peer
add address=100.3.3.10/32 exchange-mode=ike2 local-address=100.2.2.10 name=peer-office
profile=myserver.hu
/ip ipsec proposal
add auth-algorithms=sha256 enc-algorithms=aes-256-cbc name=proposal-myserver.hu pfs-
group=modp2048
/ip pool
add name=pool-branch ranges=172.16.1.100-172.16.1.200
/ip dhcp-server
add address-pool=pool-branch disabled=no interface=bridge-branch01 name=dhcp-branch01
/interface bridge port
add bridge=bridge-branch01 interface=ether2
add bridge=bridge-branch01 interface=ether3
add bridge=ipsec interface=ether5
/interface list member
add interface=ether1-internet list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
/ip address
add address=172.16.1.1/24 interface=bridge-branch01 network=172.16.1.0
add address=100.2.2.10/24 interface=ether1-internet network=100.2.2.0
/ip dhcp-server network
add address=172.16.1.0/24 dns-server=172.16.1.1 gateway=172.16.1.1
/ip dns
```

```
set allow-remote-requests=yes servers=100.2.2.2
/ip firewall filter
add action=accept chain=input comment="Allow UPD 500,4500 for IKEv2" dst-address=100.2.2.10
dst-port=500,4500 in-interface=ether1-internet protocol=udp
add action=accept chain=input comment="Allow IPSEC/ESP" dst-address=100.2.2.10 in-
interface=ether1-internet protocol=ipsec-esp
add action=accept chain=input comment="defconf: accept established,related,untracked"
connection-state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-
list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec policy" ipsec-
policy=in,ipsec
add action=accept chain=forward comment="defconf: accept established,related, untracked"
connection-state=established,related,untracked
add action=reject chain=forward comment="Reply with network-unreachable when IPSEC tunnel is
down" out-interface=ipsec reject-with=icmp-network-unreachable
add action=drop chain=forward comment="defconf:  drop all from WAN not DSTNATed" connection-
nat-state=!dstnat connection-state=new in-interface-list=WAN
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
/ip firewall mangle
add action=change-mss chain=forward comment="IKE2: Clamp TCP MSS from 172.16.2.0/24 to ANY"
ipsec-policy=in,ipsec new-mss=1360 passthrough=yes protocol=tcp src-address=172.16.2.0/24 tcp-
flags=syn tcp-mss=\
    !0-1360
/ip firewall nat
add action=masquerade chain=srcnat ipsec-policy=out,none log=yes out-interface=ether1-internet
/ip ipsec identity
add auth-method=digital-signature certificate=branch01.myserver.hu my-
id=fqdn:branch01.myserver.hu peer=peer-office remote-id=fqdn:office.myserver.hu
/ip ipsec policy
add dst-address=172.16.2.0/24 peer=peer-office proposal=proposal-myserver.hu sa-dst-
address=100.3.3.10 sa-src-address=100.2.2.10 src-address=172.16.1.0/24 tunnel=yes
/ip route
add distance=1 gateway=100.2.2.2
add comment="Prevent package leak RFC1918 class A" distance=1 dst-address=10.0.0.0/8
type=unreachable
add comment="Prevent package leak RFC1918 class B" distance=1 dst-address=172.16.0.0/12
type=unreachable
add comment="VPN to office" distance=1 dst-address=172.16.2.0/24 gateway=ipsec pref-
```

```
src=172.16.1.1
add comment="Prevent package leak RFC1918 class C" distance=1 dst-address=192.168.0.0/16
type=unreachable
/system identity
set name=branch01.myserver.hu
```

Revision #4
Created 9 January 2021 15:20:59 by Gandalf
Updated 10 January 2021 08:30:21 by Gandalf