További site-ok hozzáadása

Az alábbi leírásban már nem konkrét ip címeket használok, hanem olyan beszédes neveket mint `branch01.lan.subnet/24` vagy `branch02.router.lan.ip`. Ez elősegíti a megértést azáltal, hogy a parancsok is beszédesek lesznek (5-6 különböző hálózat számszerű címeinek észben tartása már nem egyszerű feladat.)

Új site hozzáadása

Ez egy zanzásított verzió lesz. Felsoroljuk azokat a lépéseket, amikkel egy további site-ot lehet hozzákapcsolni a központi, office site-hoz. Legyen az új site neve `branch02`.

```
; 1. Új kliens certificate készítése

/certificate add name=branch02.myserver.hu \
country=HU state=Heves locality=Eger \
    organization=myserver.hu common-name=branch02.myserver.hu \
    subject-alt-name=DNS:branch02.myserver.hu \
    key-size=4096 days-valid=1095 trusted=yes key-usage=tls-client
/certificate sign branch02.myserver.hu ca=ca.myserver.hu
/certificate export-certificate branch02.myserver.hu type=pkcs12 export-
passphrase="not_telling"

; 2. Certificate fölmásolása az új VPN branch router-jére, utána importálás
/certificate import file-name=cert_export_ca.myserver.hu.crt name="ca.myserver.hu"
/certificate import file-name=cert_export_branch02.myserver.hu.crt name="branch02.myserver.hu"
/file remove [find where name=cert_export_ca.myserver.hu.crt]
/file remove [find where name=cert_export_branch02.myserver.hu.p12]

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

; 4. ipsec phase2 proposal (proposal)
/ip ipsec proposal
```

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

; 5. ipsec peer
; branch02 router-en:
/ip ipsec peer
add exchange-mode=ike2 name="peer-office" \
   address=[/resolve office.myserver.hu] \
   profile="myserver.hu" \
   passive=yes send-initial-contact=yes
; office router-en:
add exchange-mode=ike2 name="peer-branch02" \
   address=[/resolve branch02.myserver.hu] \
   profile="myserver.hu" \
   passive=yes send-initial-contact=yes

; 6. identity
; branch02 router-n
add auth-method=digital-signature certificate=branch02.myserver.hu \
    my-id=fqdn:branch02.myserver.hu \
    peer=peer-office \
    remote-id=fqdn:office.myserver.hu
; office router-en:
add auth-method=digital-signature certificate=office.myserver.hu \
    my-id=fqdn:office.myserver.hu \
    peer=peer-branch02 \
    match-by=certificate \
    remote-certificate=branch02.myserver.hu \
    remote-id=fqdn:branch02.myserver.hu

; 7. policy
; branch02 router-en
add src-address=branch02.lan.subnet/24 dst-address=office.lan.subnet/24 \
  peer=peer-office proposal="proposal-myserver.hu" tunnel=yes
; office router-en
add src-address=office.lan.subnet/24 dst-address=branch02.lan.subnet/24 \
  peer=peer-branch02 proposal="proposal-myserver.hu" tunnel=yes

; 8. routing
```

```
; branch02 routing
/interface bridge
add name=ipsec protocol-mode=none
/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
add commend="VPN to office" distance=1 dst-address=office.lan.subnet/24 gateway=ipec pref-
src=branch02.router.ip

; office routing
add commend="VPN to branch02" distance=1 dst-address=branch02.lan.subnet/24 gateway=ipec pref-
src=office.router.ip

; correct ICMP branch02
add action=reject chain=forward comment="Reply with network-unreachable when IPSEC tunnel is
down" out-interface=ipsec reject-with=\
    icmp-network-unreachable place-before=<????>

; 9.  MTU TCP MSS

; branch02 mtu tcp mss clamping
/ip firewall mangle
add action=change-mss chain=forward new-mss=1360 \
   src-address=office.lan.subnet/24 \
   protocol=tcp tcp-flags=syn tcp-mss=!0-1360 \
   ipsec-policy=in,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from
office.lan.subnet/24 to ANY"
```

Teljesen összekapcsolt hálózatok

A korábban leírt módszerrel bármikor hozzá tudsz adni több site-ot, és a különböző site-ok között VPN kapcsolatokat kialakítani. Három site esetén akár még előnyös is lehet az, hogy minden site minden site-tal kapcsolatban van. ("Fully connected network"). Ennek az az előnye, hogy bármely site elérhetetlensége esetén az összes többi kommunikálni tud egymással. A gondok akkor

kezdődnek, amikor a site-ok száma elkezd növekedni. Egy 10 site-ból álló hálózatnál már 45 alagutat kellene kiépíteni ahhoz, hogy minden site mindegyik másikat lássa.

Csillag topológia

Helyette választhatunk egy csillag topológiát: minden site az office -hoz csatlakozik, és a branch-ek közöti forgalmat az office továbbítja. Ennek van egy olyan előnye is, hogy a telephelyek közötti forgalmat egyetlen egy helyen, az office tűzfalával meg lehet szűrni. A nyilvánvaló hátránya az, hogy a csillag közepe egy SPOF, és természetesen az összes hálózati forgalom áthalad rajta, ezért nagyobb a hálózat terhelése.

Ezt a fajta összekötést úgy érjük el, hogy újabb ipsec policy-k hozzáadásával rávesszük a telephelyeket arra, hogy a "többi" telephely irányába menő forgalmat is az alagúton küldjék át.

branch02 gépen

```
/ip route
add comment="VPN to branch01 through office" distance=1 \
  dst-address=branch01.lan.subnet/24 \
  gateway=ipsec \
  pref-src=branch02.router.lan.ip

/ip ipsec policy
add peer=peer-office proprosal=proposal-myserver \
  src-address=branch02.lan.subnet/24 \
  dst-address=branch01.lan.subnet/24 \
  tunnel=yes
```

branch01 gépen:

```
/ip route
add comment="VPN to branch02 through office" distance=1 \
  dst-address=branch02.lan.subnet/24 \
  gateway=ipsec \
  pref-src=branch01.router.lan.ip

/ip ipsec policy
add peer=peer-office proprosal=proposal-myserver \
  src-address=branch01.lan.subnet/24 \
  dst-address=branch02.lan.subnet/24 \
  tunnel=yes
```

office01 gépen:

```
/ip ipsec policy
add peer=peer-branch01 proprosal=proposal-myserver dst-address=branch01.lan.subnet/24 src-address=branch01.lan.subnet/24 tunnel=yes
add peer=peer-branch02 proprosal=proposal-myserver dst-address=branch02.lan.subnet/24 src-address=branch01.lan.subnet/24 tunnel=yes
```

Egyéb más topológiák

A fent leírtak alapján bárki kialakíthat magának más topológiákat. Például csillagok csillagokba kötve stb. Általában véve igaz, hogy ilyen nagy számú telephely összekötésére másfajta megoldást érdemes választani. Például lehet telepíteni szerver terembe magas rendelkezésre állású, gyors hálózati kapcsolattal rendelkező StrongSwan VPN szervereket, és ezeken keresztül redundáns módon összekötni a telephelyeket. Ez azonban már túlmutat ennek a leírásnak a keretein.

Revision #7
Created 10 January 2021 08:32:18 by Gandalf
Updated 10 January 2021 10:24:37 by Gandalf