Tűzfal beállítások

Szeretném fölhívni a figyelmet arra, hogy a korábbi szakaszokban leírt példa hálózatban az office és branch01 router-ek semmiféle tűzfal szabályt nem tartalmaznak az internet felől érkező támadások kivédésére. Ha például egy támadó képes IP Spoofing felhasználásával kívülről az internet irányából küldeni olyan csomagokat, amiknek a forrás- és célcíme az office illetve branch01 címtartományában van, akkor azzal rá tudja venni a router-eket, hogy ezeket a csomagokat is enkapszulálják, titkosítsák és küldjék át az alagúton. Mivel a támadó ismeri az eredeti (később enkapszulált) csomagok tartalmát, ezért az adatforgalom megfigyelésével lehetősége van egy olyan támadás végrehajtására, ahol tetszőleges titkosítatlan adathoz meg tudja határozni a titkosított párját. Ez az úgynevezett Known-Plaintext attack, ami nagyságrendekkel egyszerűbben visszafejthetővé teszi a kulcsokat, ezáltal magas biztonsági kockázatot jelent.

Alább leírok egy minimális konfigurációt ami megmutatja, hogy a példában leírt site-to-site kapcsolatnál milyen szabályokat kell hozzáadni ahhoz, hogy a VPN alagút védett és működőképes legyen.

> Az alábbiakat semmiképp ne alkalmazd vakon! A Te konkrét feladatodnak megfelelően kell módosítani ezeket a szabályokat. Szinte biztos, hogy Te konkrét esetedben ez a minta változtatás nélkül nem alkalmazható. Figyelmeztetve lettél.

Először listába szervezzük a WAN és LAN interface-eket. Midkét router-en az ether1 interface kapcsolódik az ISP-hez. Ezt hangsúlyozandó, átnevezzük ether1-internet -re:

```
/interface
set name=ether1-internet [find name=ether1]
/interface list
add name=LAN
add name=WAN
/interface list member
add list=WAN interface=ether1-internet
add list=LAN interface=ether2
add list=LAN interface=ether3
add list=LAN interface=ether4
add list=LAN interface=ether5
```

Az office router-en ezen felül a következőket állítjuk be:

```
/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=accept chain=forward in-interface-list=LAN src-address=172.16.2.0/24
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 nat
add action=masquerade chain=srcnat out-interface=ether1-internet
```

A branch01 oldalon ennek teljesen a tükörképe van. Csak a WAN cím módosul, és a privát alhálózatok címe cserélődik föl:

```
/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=accept chain=forward in-interface-list=LAN src-address=172.16.1.0/24
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 nat
add action=masquerade chain=srcnat out-interface=ether1-internet
```

A beállítások után ne felejts el újra tesztelni! Nézd meg, hogy az egyes alhálózaton levő gépekből ki mit lát: azonos alhálózatban, másik alhálózatban, interneten stb.

Néhány érdekesség:

- Rögtön az input chain legelején engedélyezzük a bejövő csomagokat az UDP/500 és UDP/4500 portokon. Ez szükséges ahhoz, hogy az IKE démonok végre tudják hajtani az első és második fázist. Ezen keresztül azért nehéz támadást véghezvinni, mert az azonosításhoz szükség van a tanúsítványokra.
- Az input és forward chain-ek legelején elfogadjuk az összes, internet irányából érkező ipsec-esp csomagot. Ez azért nem jelent biztonsági kockázatot, mert ezeknek a csomagoknak a kicsomagolása közben az érvénytelen ellenőrző összeggel rendelkező csomagok automatikusan eldobásra kerülnek.
- Ami ezután van az csak a szokásos: engedjük az ICMP-t, eldobjuk az érvénytelen csomagokat, eldobunk minden más bejövőt ami nem a LAN irányából érkezik, eldobunk minden továbbítandó csomagot (kivéve a port forward-hoz használt dsnat-on átesetteket) stb. Igazából a maradék szabályok kb. ugyan azok, mint amiket egy alapértelmezett RouterOS konfiguráció reset után megtalálsz bármelyik MikroTik eszközben.

Revision #3
Created 2 January 2021 19:25:51 by Gandalf
Updated 9 January 2021 15:20:50 by Gandalf