Meglevő hálózat ellenőrzése

VPN kapcsolat kialakítása előtt feltétlenül teszteld le, hogy a kezdeti (VPN nélküli) állapotban minden gép lát minden másikat az alhálózatokon belül, plusz azt is hogy minden gép lát minden nyilvános címmel rendelkező gépet.

> Ha ezeket a teszteket nem végzed el, akkor lehet hogy egy olyan környezetben kezded el kialakítani a VPN hálózatot, ahol az nem is lehetséges. Ez nagyon meg tudja nehezíteni a hibák lokalizálását és elhárítását.

branch01 -en belül tesztek

A kezdeti állapotban a branch01-en belül mindenki lát mindenkit. Az alábbi képen a PC1 gépről a következőket próbálom elérni:

- Saját LAN oldali router 172.16.1.1
- Saját branch01 router WAN publikus címe 100.2.2.10
- Az internetet szimuláló router-en több cím: 100.2.2.2, 100.3.3.3 és 100.4.4.4
- Az office router WAN publikus címe 100.3.3.10

```
PC1> ping 172.16.1.1 -c 1
84 bytes from 172.16.1.1 icmp_seq=1 ttl=64 time=0.260 ms

PC1> ping 100.2.2.10 -c 1
84 bytes from 100.2.2.10 icmp_seq=1 ttl=64 time=0.392 ms

PC1> ping 100.2.2.2 -c 1
84 bytes from 100.2.2.2 icmp_seq=1 ttl=63 time=0.978 ms

PC1> ping 100.3.3.3 -c 1
84 bytes from 100.3.3.3 icmp_seq=1 ttl=63 time=0.677 ms

PC1> ping 100.4.4.4 -c 1
84 bytes from 100.4.4.4 icmp_seq=1 ttl=63 time=0.646 ms

PC1> ping 100.3.3.10 -c 1
84 bytes from 100.3.3.10 icmp_seq=1 ttl=62 time=1.383 ms
```

Ezek ICMP ping tesztek. (Ha nem vagy benne biztos hogy mi az az ICMP, akkor olvasd el ezt.) Sok esetben a TCP illetve UDP kapcsolatokat korlátozzák az úton levő tűzfalak, miközben az ICMP csomagokat átengedik. Ha van rá lehetőséged, akkor végezd el ezeket a teszteket TCP és UDP protokollal is. Itt nem másolom be az összes tesztet, de a `branch01` router-jéről is látni a Windows10-1 és PC1 gépeket, plusz a Windows10-1 gépről is látni a PC1 és `branch01` router gépeket, ezen felül az "interneten" levő összes "nyilvános" címet is.

office -on belüli tesztek

Nem győzőm hangsúlyozni a tesztek fontosságát. Nagyon hasonlókat tesztelünk a PC2 gépről is:

- Saját LAN oldali router 172.16.2.1
- Saját branch01 router WAN publikus címe 100.3.3.10
- Az internetet szimuláló router-en több cím: 100.2.2.2, 100.3.3.3 és 100.4.4.4
- Az branch01 router WAN publikus címe 100.2.2.10

```
PC2> ping 172.16.2.1 -c 1
84 bytes from 172.16.2.1 icmp_seq=1 ttl=64 time=0.540 ms

PC2> ping 100.3.3.10 -c 1
84 bytes from 100.3.3.10 icmp_seq=1 ttl=64 time=0.327 ms

PC2> ping 100.2.2.2 -c 1
84 bytes from 100.2.2.2 icmp_seq=1 ttl=63 time=0.646 ms

PC2> ping 100.3.3.3 -c 1
84 bytes from 100.3.3.3 icmp_seq=1 ttl=63 time=0.588 ms

PC2> ping 100.4.4.4 -c 1
84 bytes from 100.4.4.4 icmp_seq=1 ttl=63 time=0.595 ms

PC2> ping 100.2.2.10 -c 1
84 bytes from 100.2.2.10 icmp_seq=1 ttl=62 time=1.072 ms
```

branch01 és office közötti tesztek

Ami nyilvánvalóan nem működik, az az `office1` és a `branch01` hálózat közötti kapcsolat. A `branch01` router-je nem tud az `office` belső hálózatáról és fordítva. Az internetet jelképező router pedig nem tud egyik belső céges hálózatról se.

```
PC1> ping 172.16.2.1 -c 1
*100.2.2.2 icmp_seq=1 ttl=63 time=0.730 ms (ICMP type:3, code:0, Destination network unreachable)

PC1> ping 172.16.2.10 -c 1
*100.2.2.2 icmp_seq=1 ttl=63 time=0.713 ms (ICMP type:3, code:0, Destination network unreachable)
```

A hibát ("elérhetetlen hálózat") mindig az internetet jelképező router küldi vissza. Mivel a helyi (`branch01` vagy `office`) router nem tudja hogy hol van a cél cím, ezért a default route (internet) felé továbbítja a csomagokat. Az internetet jelképező router se tudja hogy ezek hol vannak (privát LAN-ok belső címei), ezért visszaküldi hogy a célhálózat nem elérhető.

A VPN kapcsolat kialakításának pont ez az egyik célja. Azt szeretnénk elérni, hogy a két telephely gépei lássák egymást. A másik célja természetesen az, hogy ez a kapcsolat biztonságos legyen. Az interneten keresztül utazó adatokat ne tudja bárki megnézni, visszafejteni és bizalmas adatokhoz hozzájutni.

Revision #5
Created 2 January 2021 18:02:19 by Gandalf
Updated 9 January 2021 13:27:53 by Gandalf