Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és alkalmazás-üzemeltető technikus

***száma:*** 5-0612-12-02

**VIZSGAREMEK**  
**Szász Tamás István korház hálózatának teszteléses dokumentációja**

Fazekas Gábor János, Kun Leon

2/14B

Budapest, 2024.

Tartalom

[Hálózat ismertetése 3](#_Toc164004725)

[Kék terület 4](#_Toc164004726)

[VTP(Vlan Trunk Protocol) 4](#_Toc164004727)

[PAgP (Port Aggregation Protocol) 5](#_Toc164004728)

[Port biztonság (Port-security) 6](#_Toc164004729)

[Feszítőfa protokoll (Spanning Tree Protocol) 7](#_Toc164004730)

[DHCP-Snooping 8](#_Toc164004731)

[Lila terület 8](#_Toc164004732)

[GRE Alagút 8](#_Toc164004733)

[Sárga terület 10](#_Toc164004734)

[ZPF 10](#_Toc164004735)

[Piros terület 13](#_Toc164004736)

[ASA 13](#_Toc164004737)

[Szürke terület 14](#_Toc164004738)

[HSRP 14](#_Toc164004739)

[NAT 16](#_Toc164004740)

[ACL 17](#_Toc164004741)

[Szerverek 19](#_Toc164004742)

[Tanúsítvány 26](#_Toc164004743)

## Hálózat ismertetése

Cégünket a Szász Tamás István kórház bízta meg, a több területre eső hálózatuk megtervezésével, illetve megvalósításával. Cégünk a kor legmodernebb eszközeit használva építette ki a hálózatot, mely a legbiztonságosabb módon lett felkonfigurálva

## Kék terület

### VTP(Vlan Trunk Protocol)

A VTP lehetővé teszi egy vagy több VLAN hozzáadását, átnevezését vagy törlését egyetlen kapcsolón (a szerveren), amely ezt az új konfigurációt továbbítja a hálózat összes többi kapcsolójára (kliensekre).

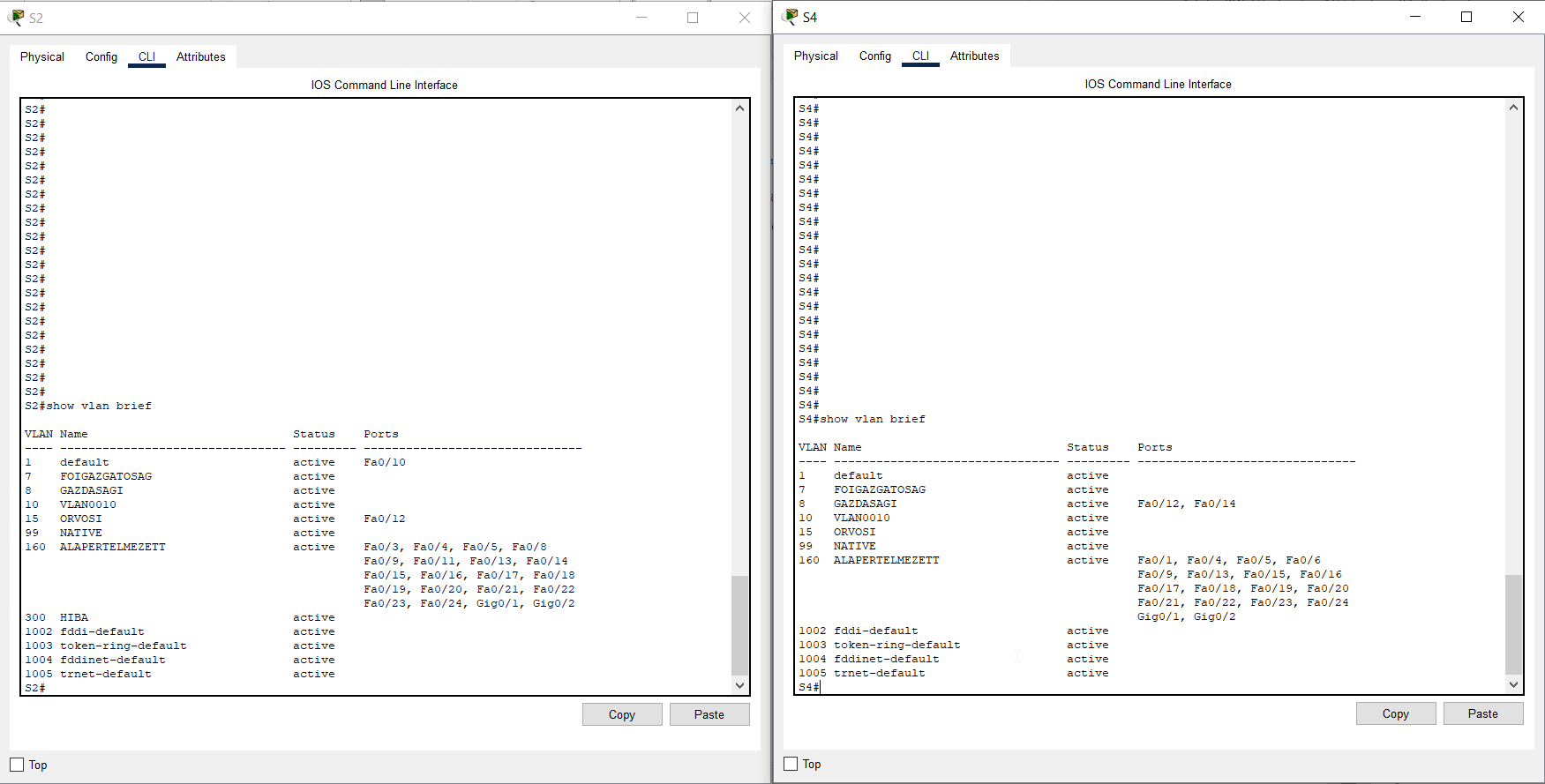
A VTP hibamentesen működik, addig, ameddig nem adunk meg eltérő információkat, a kliensnek és a szervernek.  
 A tesztelés érdekében, az egyik kliensen megváltoztattuk a domain címet.



1. ábra - VTP domain megváltoztatása a kliensen

Ekkor egy ún. **domain-mismatch** hibát kapunk, viszont a hálózat a hiba előtti beállításokkal, továbbra is működik.

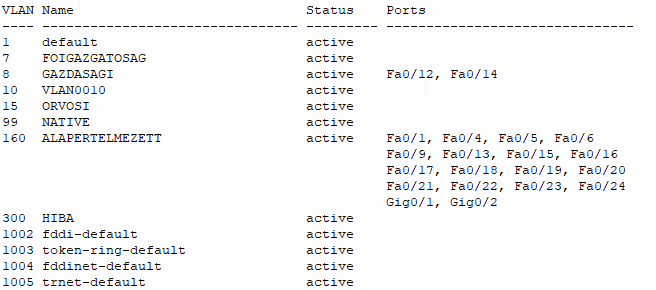
2. ábra - Domain egyezés hiba a VTP-n

 A domain név megváltoztatása után, létrehozunk egy vlan-t a szerver switchen, HIBA névvel.

3. ábra - show vlan brief parancs kimenetele VTP esetén

A fenti fotón láthatjuk, hogy az S2-Switch, ami azonos domain címmel rendelkezik mint a szerver, megkapta a HIBA nevű vlan, viszont az S4, amin átállítottuk a domain címet hiba.hu-ra, nem kapta meg.

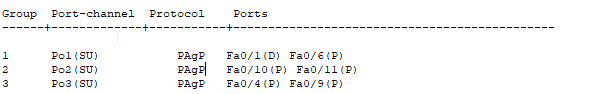
Miután a S4-en visszaállítjuk a domain címet, a szerverrel azonos domain címre (szaszkh.hu), az S4 kliens azonnal megkapja, a hiányzó VLAN-t



### PAgP (Port Aggregation Protocol)

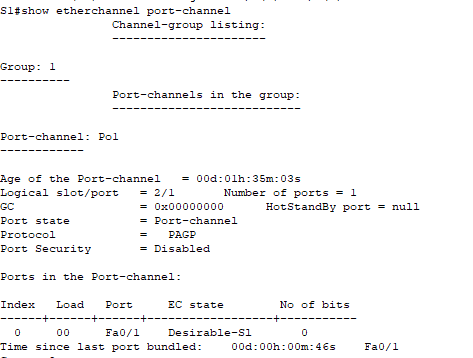
A PAgP a Cisco saját fejlesztésű protokollja, mely az EtherChannel kapcsolatok automatikus létrehozását segíti. Használata esetén a kapcsolók PAgP-csomagokkal egyeztetnek a portok között az EtherChannel kialakításához. Ha a PAgP megfelelő Ethernet portokat talál, összefogja azokat egy EtherChannel-be, amely ezután egyedi portként vesz részt a feszítőfában.

A PAgP lényege hogy ha az egyeik kábel megsérül vagy lekapcsolódik akkor a másik csatlakoztatott kábel továbbra is működteti a hálózatot.



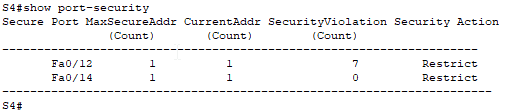
A fenti képen az S1 azaz a szerver Switchhez kapcsolódó port-channelek láthatóak

A PAgP csak akkor működik helyesen, ha jól konfiguráljuk fel. A mi esetünkben S1-S2 között az S1 fa0/6-os interfészen channel-group 1 mode desirable parancs van kiadva, ami a PAgP-t állítja be, amíg a másik oldalon channel-group 1 mode auto Aminek köszönhetően az S2 fa0/6 interfésze felveszi a másik oldalon megadott beállítást.

A tesztelés érdekében mindkét oldalt módját auto-ra állítottuk, így egyik oldal se kezdi el a PAgP csomagok egyeztetését ennek köszönhetően a switchek csak az egyik interfészen keresztül kommunikálhatnak

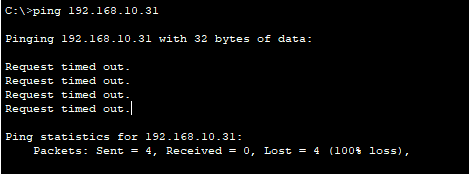
### Port biztonság (Port-security)

A port-security megvédi a hálózatot az ismeretlen MAC címek elárasztásától. Cégünk a sticky módszert használta a MAC-címek felismerésére. A három violation módból a restrictet választottuk ami amelett hogy eldobj a keretet, naplózza az eszköz MAC-címét. A tesztelés érdekében az fa0/12-es interfészre csatlakoztattunk egy új gépet. Mint látható a switch hétszer észlelt sértést és dobta el a csomagokat.

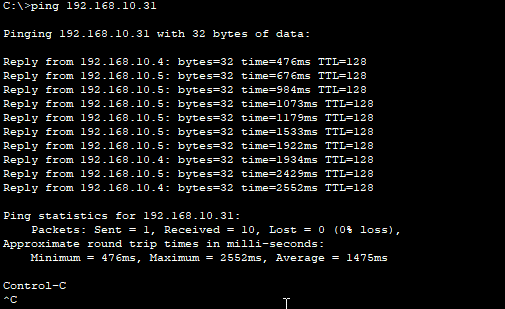


4. ábra- show port security parncs kimenete

### Feszítőfa protokoll (Spanning Tree Protocol)

A feszítőfa protokollt a redundancia növelése és a szórási viharok (broadcast-storm) elkerülése érdekében alkalmaztuk. Rapid-PVST+ használata esetén így néz ki egy broadcast üzenet. Látható, hogy a feszítőfa nem engedi el a szórásos üzentet.

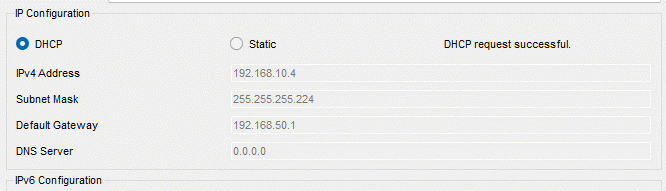
A tesztelés érdekében kikapcsoltuk a feszítőfát a switcheken majd küldtünk egy szórásos üzenetet az egyik eszközről ezzel szórási vihart kialakítva.

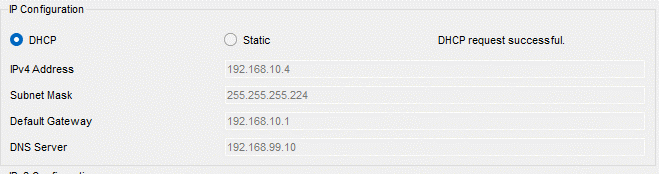


A képen látható, hogy a csomag a végtelenségig vagy megszakításig kering a switchek között.

### DHCP-Snooping

A DHCP-Snooping funkciója a DHCP-üzenetek szűrése. Nem engedi át azokat DHCP-üzeneteket, amik nem megbízható portrol küldtek.

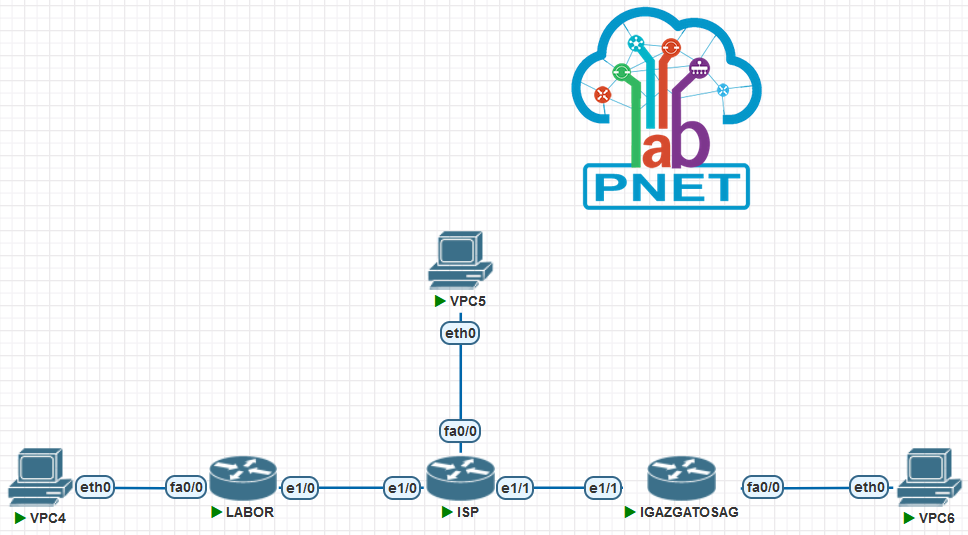
A tesztelés érdekében a Vlan 15-höz beraktunk egy „betörő” DHCP szervert, ami más átjárót ad, mint a rendes DHCP szerverünk.

Ha megfelelően beállítjuk a DHCP snoopingot akkor a rendes szerverről kapja meg az ip-címet

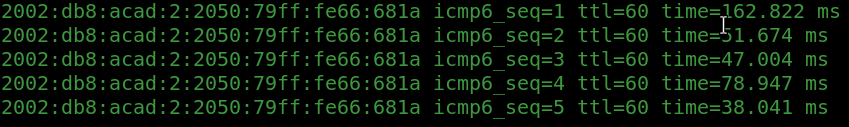
## Lila terület

### GRE Alagút

A GRE Alagút egy olyan virtuális pont-pont kapcsolat, amely fizikailag nem létezik, de a forgalomirányítás számára egy létező útvonalat biztosít a (szoftveres,virtuális) interfészek összekapcsolásával.

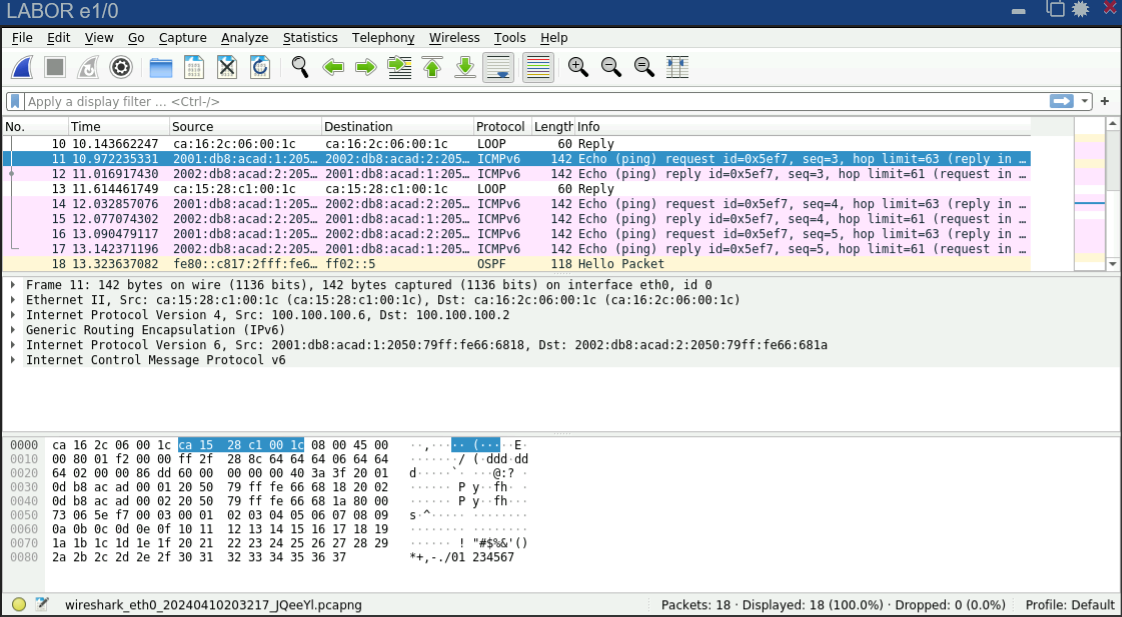
Mivel a Packet Tracer nem teljesen támogatja a GRE protokollt, ezért az Tunnel-t PNETLAB segítségével mutatjuk be. Az egyszerűbb bemutatás érdekében, csak a topológia azon részét szemléltetjük, melyen keresztül megy a GRE alagút.

ábra 5 - GRE Topológia

A GRE Alagút működésétét egy ping, és a wireshark nevű csomagelemző program segítségével szemléltetjuk.

ábra 6 - GRE IPv6 ping

Ahogyan a LABOR számítógépének terminálja is mutatja, a ping gond nélkül megérkezett, azonban ez az információ nem tartalmazza, hogy mindez a GRE Alagúton keresztül történt. Erre a célra alkalmas a wireshark, mely bővebb információkkal szolgál.



ábra 7 - Wireshark GRE

Ahogyan a képen is látható, a ping IPv4-en keresztül, egy Generic Routing Encapsulation, azaz egy GRE csomagon keresztül lép ki a hálózatból, és abban is érkezik meg.

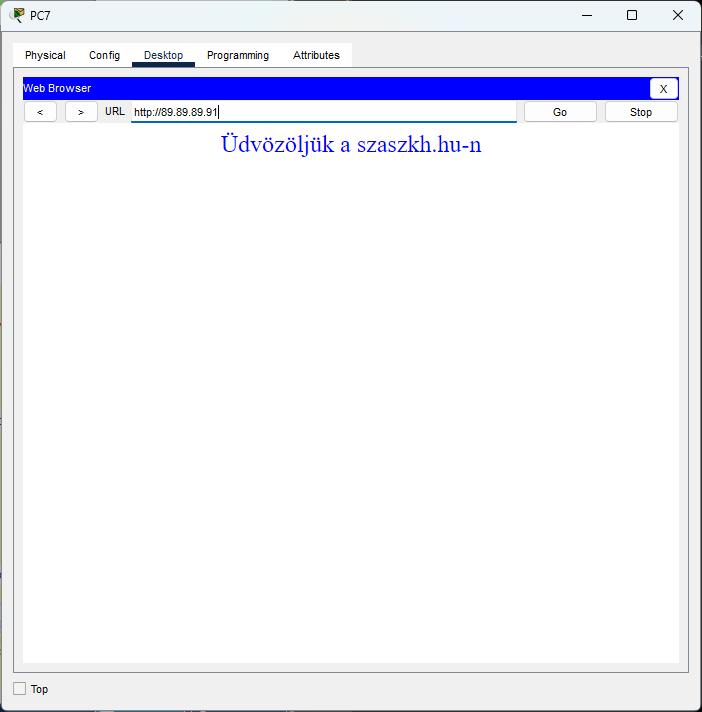
## Sárga terület

### ZPF

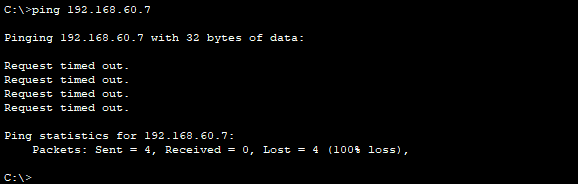
A Cisco Zone-Based Policy Firewall (ZPF) egy hálózati biztonsági megoldás, amely a hálózatot különböző biztonsági zónákra osztja. A ZPF szabályokat határoz meg a zónák közötti forgalomra, így védve a hálózatot a jogosulatlan hozzáféréstől, támadásoktól és behatolásoktól.

A ZPF célja hogy szűrje forgalmat a területen. A területen csak a http és https csomagok küldése engedélyezett.

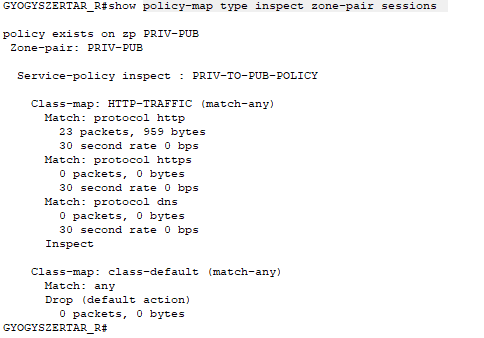
Mint látható a web szerveren található weboldalt el lehet érni.



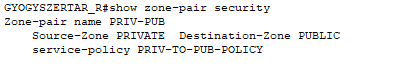
Viszont ICMP és egyéb csomagokat nem enged át a ZPF



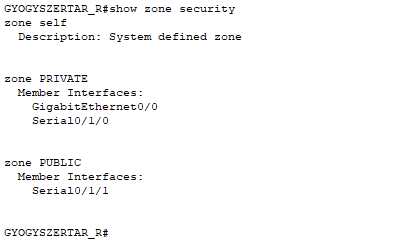
A show policy-map type inspect zone-pair sessions parancs kiadásával láthatjuk a policy-map-et amiben láthatóak a szűrt protokolok és a küldött csomagok száma.



A show zone-pair security parancs kiadásával megtekinthetjük a zóna párokat amiket létrehoztunk. Itt látható a forrás zóna ami jelen eset a PRIVATE ami a belső hálozat és a cél hálózatot ami a PUBLIC zóna



A show zone security paranccsal láthatjuk a zónákat és azok interfészeit.

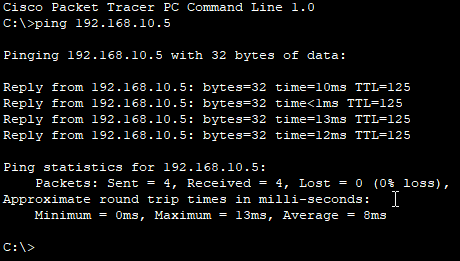


## Piros terület

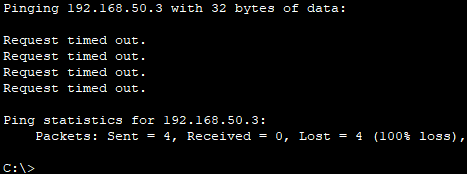
### ASA

A Cisco ASA egy többfunkciós biztonságiőrként működik a hálózat számára. Végrehajtja a biztonsági irányelveket, és felügyeli a bejövő és kimenő forgalmat, megvédi a hálózatot az illetéktelen hozzáféréstől és a rosszindulatú szoftverektől.

Feladata, hogy kívülről ne érjék el a belső hálózatot, viszont a belső hálózat minden mást problémamentesen elérjen.

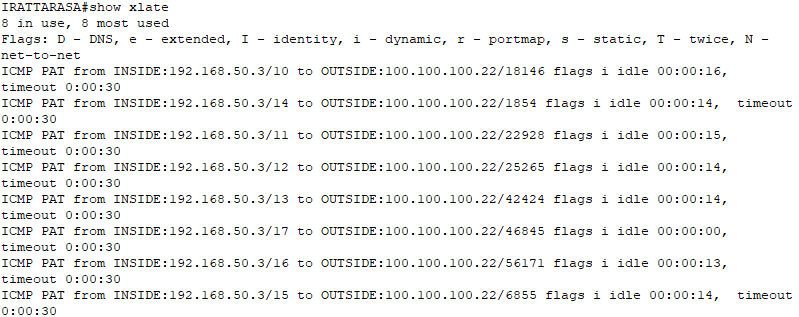


ábra 8 - ASA belső hálózat - ping

 Mint látható a belső hálózat képes kommunikálni a külső hálózattal, azonban fontos, hogy a külső hálózat erre ne legyen képes a lentebb látható kép ezt tökéletesen szemlélteti.

ábra 9 - ASA külső hálózat - ping

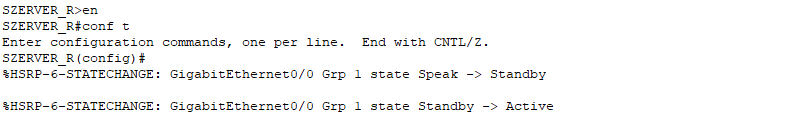
Ezen funkció hibamentes működése a Dokumentációban kivesézett Class-, illetve Policy-Map-nek köszönhető.

A területen használt számítógép privát címmel nem képes kommunikálni a külső hálózatokkal, Dinamikus NAT-ot alkalmaztunk a területen. A Dinamikus NAT-nak köszönhetően, az ASA egy a külső interfészen elérhető nyilvános címre fordítja le a privát címet, melynek köszönhetően képes kommunikálni a külső hálózattal. Ezen fordításokat lentebb megtalálható kép mutajta

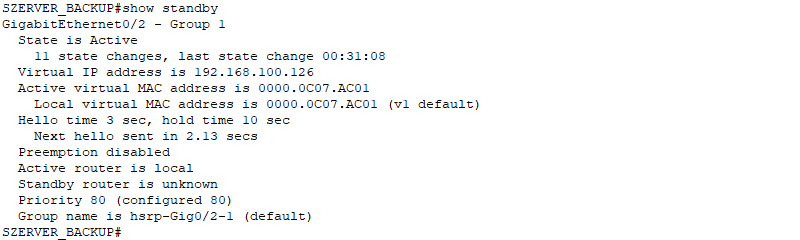
ábra 10 - show xlate parancs kimenetele

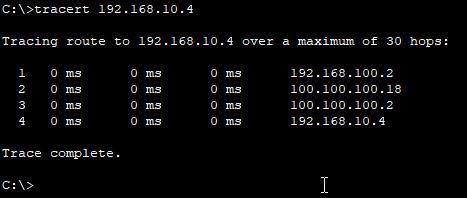
## Szürke terület

## HSRP

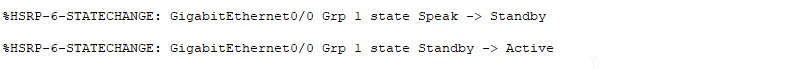
Az HSRP, vagyis a Hot Standby Router Protocol, egy Cisco által kifejlesztett redundancia növelő protokoll, amely lehetővé teszi a hálózati eszközök gyors átvételét, ha az elsődleges eszköz meghibásodik. Az HSRP egy virtuális IP-címet és MAC-címet használ, amelyet a hálózati eszközök egy csoportja oszt meg, így biztosítva a folyamatos hálózati elérhetőséget és a forgalom zavartalan átirányítását.

Mint látható, a forgalomirányító, bekapcsoláskor aktív állapotra vált. Ezzel szemben, a SZERVER\_BACKUP pedig passzívra.

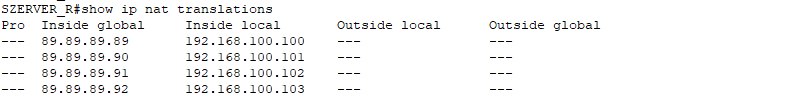
Ha azonban az aktív router áramkimaradás vagy egyéb hiba okán leáll, akkor a BACKUP router veszi át az aktív szerepet, és biztosít elérést a végberendezéseknek.

Ahogyan a kép is mutatja, a show standby parancsot kiadva láthatjuk, hogy a **SZERVER\_BACKUP** aktív állapotba lépett.

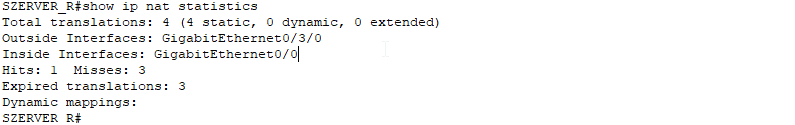
A szerveren a tracert parancs kiadásával láthatjuk, hogy a ping a BACKUP forgalomirányítón keresztül jutott el a másik hálózatba.

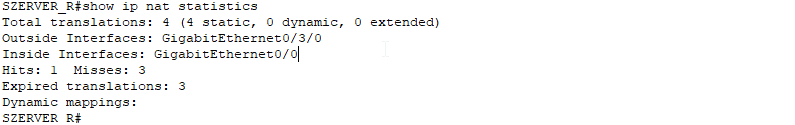
Miután a probléma helyreállt, tehát visszakapcsolt a fő forgalomirányító, látható, hogy az aktív szerepet automatikusan visszavette

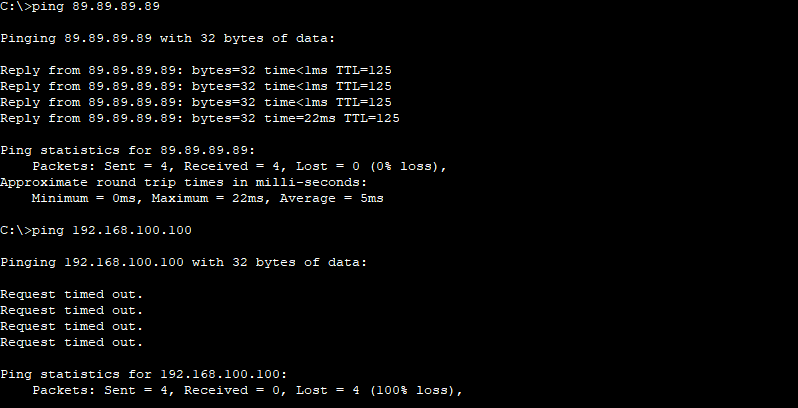
### NAT

A NAT lényege, hogy a belső hálózatban lévő eszközök IP címeit a külső hálózat felé lefordítja más IP címekre. Ez a fordítás lehetővé teszi, hogy a belső hálózatban lévő eszközök az internethez kapcsolódjanak anélkül, hogy nyilvános IP címre lenne szükségük. A statikus NAT-ot akkor használjuk, ha a belső hálózatban lévő egy adott eszközt a külső hálózatról is el kell érni.

A show ip nat translations parancsot kiadva láthatjuk, hogy mely belső címeket, milyen külső címekre fordítja a NAT. A képen látható, hogy a 89.89.89.0-ás külső címen érik el más hálózat végberendezései



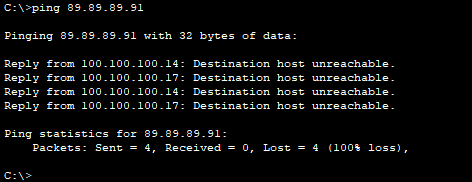
A fontosabb statisztikák érdekében, elengedhetetlen a show ip nat statistics parancs használata, hiszen itt kapunk pontos információt arról, hogy hányszor sikerült a címfordítás, illetve hányszor nem.

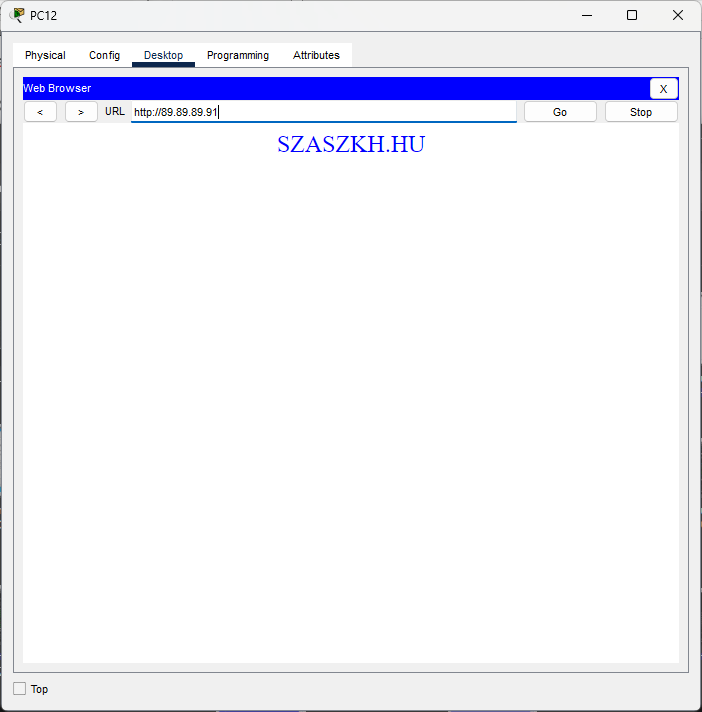
A tesztelés érdekében az igazgatóság gépéről küldünk egy pinget a PDC szerverre. A képen látható, hogy a PC a szervert, a publikus címen tökéletesen eléri, míg a privát címen nem.

### ACL

Az ACL célja a hálózati forgalmak szabályozása. Lehetővé teszi a hálózati adminisztrátorok számára, hogy meghatározzák, hogy mely forrás IP-címek férhetnek hozzá a cél IP-címekhez és portokhoz, és melyek nem. Az ACL-eket tűzfalakon, útválasztókon és más hálózati eszközökön lehet konfigurálni. Az ACL-eknél használhatunk azonosítókat és neveket is ezeket hívjuk nevesített ACL-nek



A tesztelés érdekében küldtünk egy pinget az egyik gépről az egyik szerverre látható, hogy a ping sikertelen.

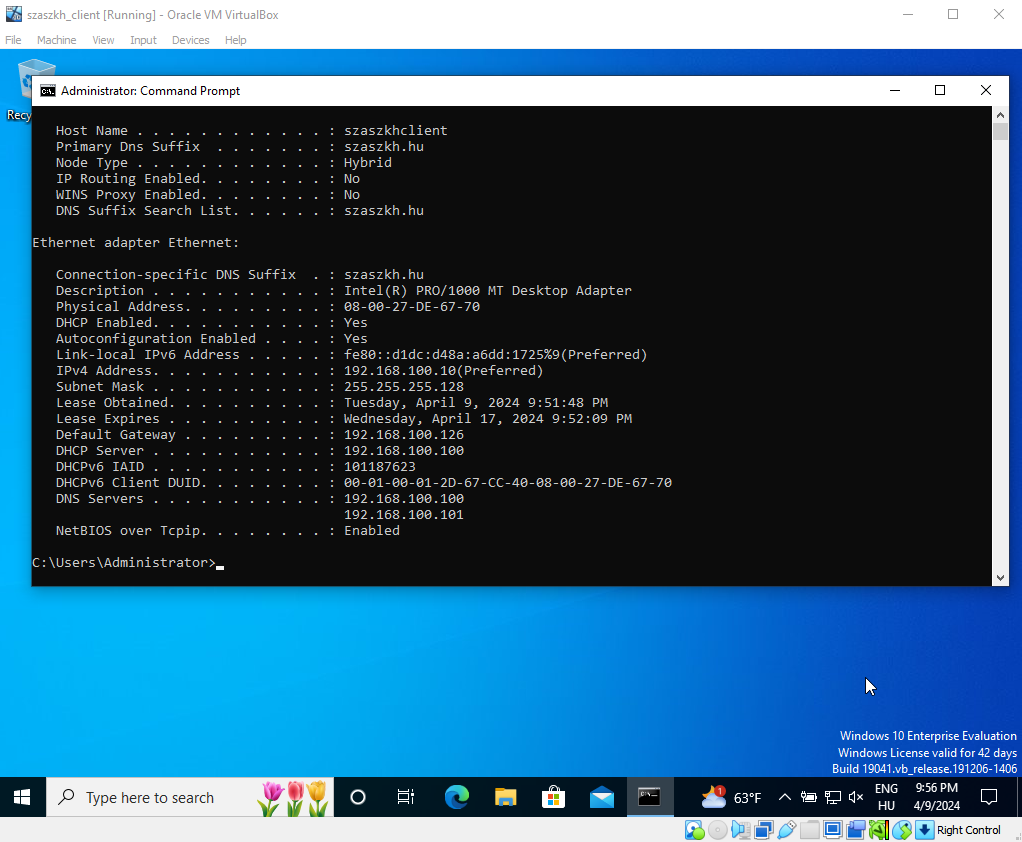
Mint látható a szerveren található weboldalt az ACL ellenére probléma mentesen el lehet érni

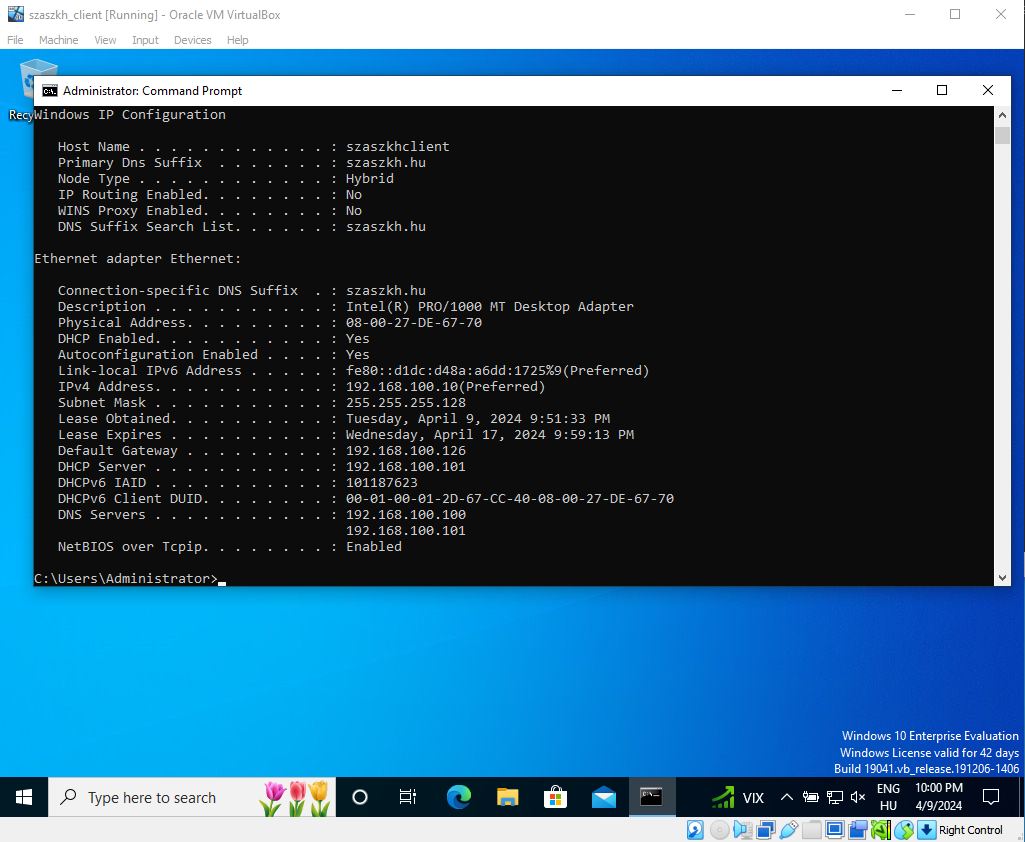
### Szerverek

#### PDC-BDC Szerver

A területen megtalálható szerverek mindegyike fontos feladatokat lát el.

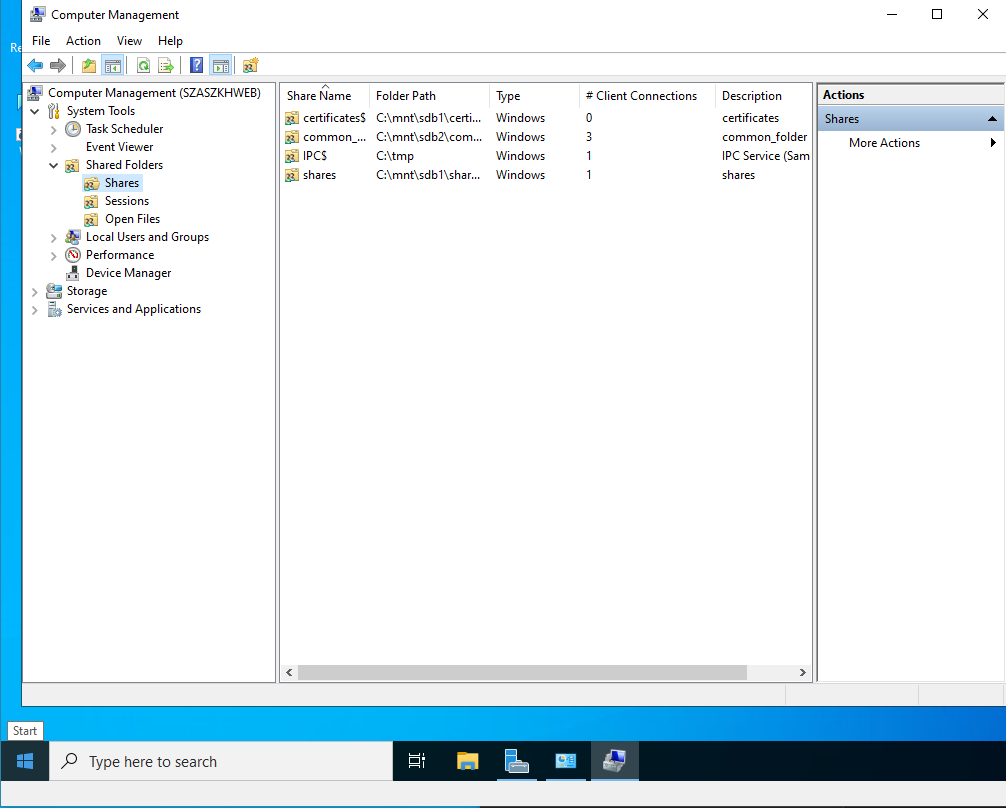
A szürke területen helyet kapott egy Windows alapú **PDC**, **AD**, illetve **DNS** szerver, egy szintén Windows (Core) alapú **BDC** (Backup Domain Controller) szerver és egy Linux (CLI) alapú **File**, **Web**, és **Print**szerver.

A PDC szerver biztosítja a domainhez való hozzáférést a felhasználók számára. Fontos, hogy ha bármi okból leáll ez a szerver, a domain továbbra is a dolgozók rendelkezésére álljon. Ezen okból kifolyólag, cégünk egy **BDC** szervert üzemeltet a kórház számára, mely továbbra is biztosít hozzáférést a **PDC** leállása esetén.

Mint látható, alap esetben 192.168.100.100-as IP-címmel rendelkező szerver (PDC Szerver) biztosít IP címeket a klienseknek. Abban az esetben, ha a PDC szerver leáll, a BDC átveszi a szerepét.

Ezen a képen látható, hogy a kliens továbbra is rendelkezik internet hozzáféréssel, és a domainhez tartozik. Ez a BDC szervernek köszönhető.

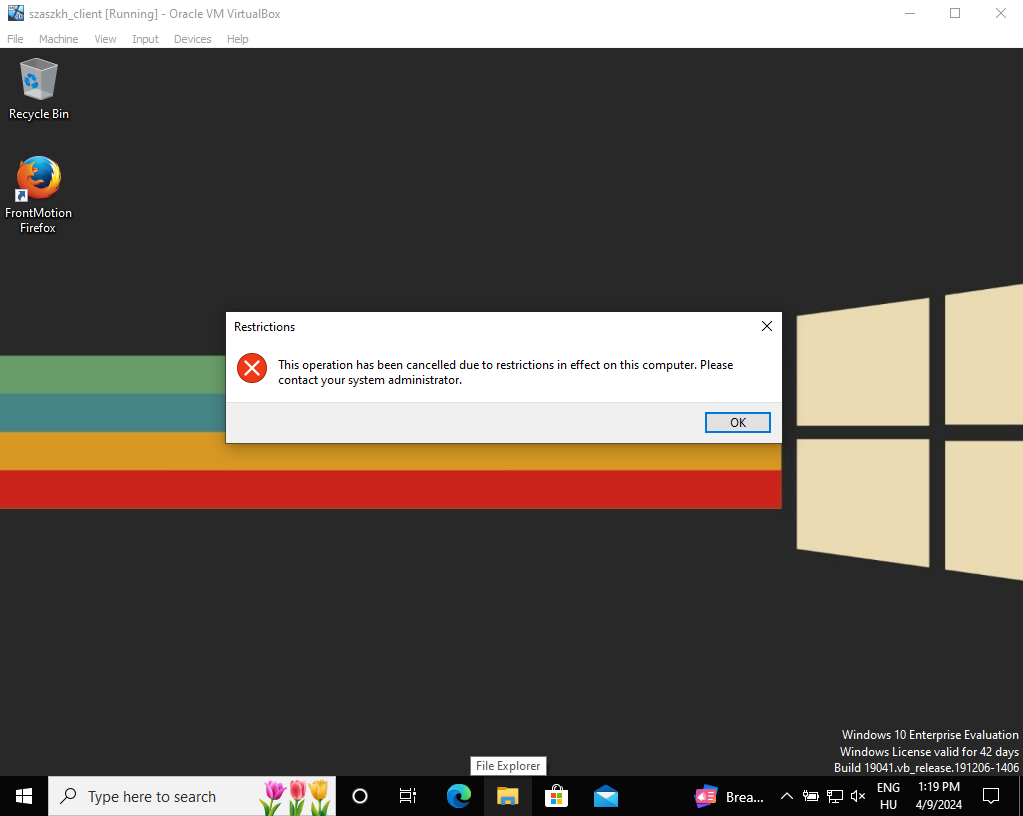
#### DNS

A **DNS**-nek köszönhetően a szervereket könnyebb formában is eléri az Admin, ahelyett, hogy IP-címeket írna be. Ha a rendszergazda távolról hozzá szeretne férni a Webszerverhez, elég csak a megadott hosztnevet beírnia IP-cím helyett.

A képen látható, hogy a rendszergazda a „szaszkhweb” hosztnevet megadva rácsatlakozott a Linux szerverre, melyen a megosztott mappákat ellenőrízte.

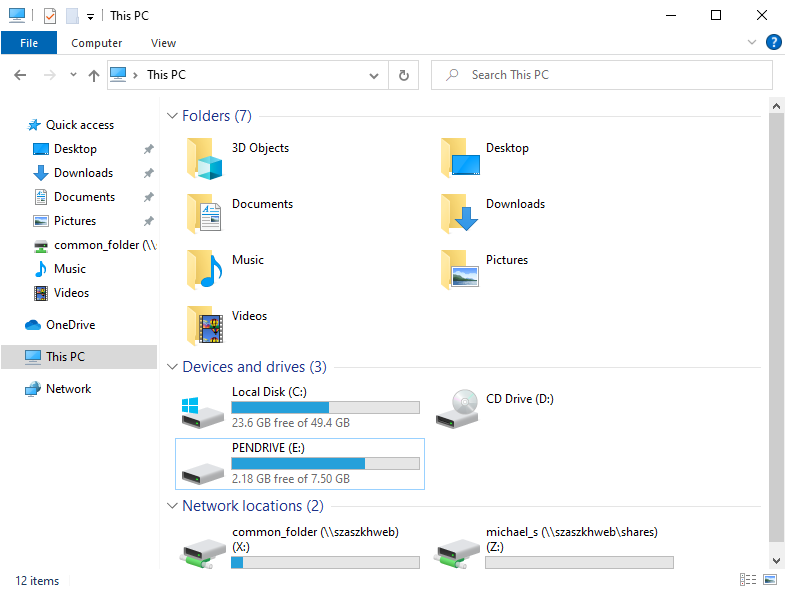
#### Csoportházirendek

A csoportházirendek segítségével korlátozhatjuk, hogy a felhasználók bizonyos funkciókat elérjenek/kárt tegyenek a számítógépben, Ilyen funkciók például a **CMD vagy a Regedit**. Ha egy hozzáértő felhasználó hozzáfér ezekhez a funkciókhoz, módosíthat olyan beállításokat, mely a gátolhatja a számítógép rendeltetésszerű működését.

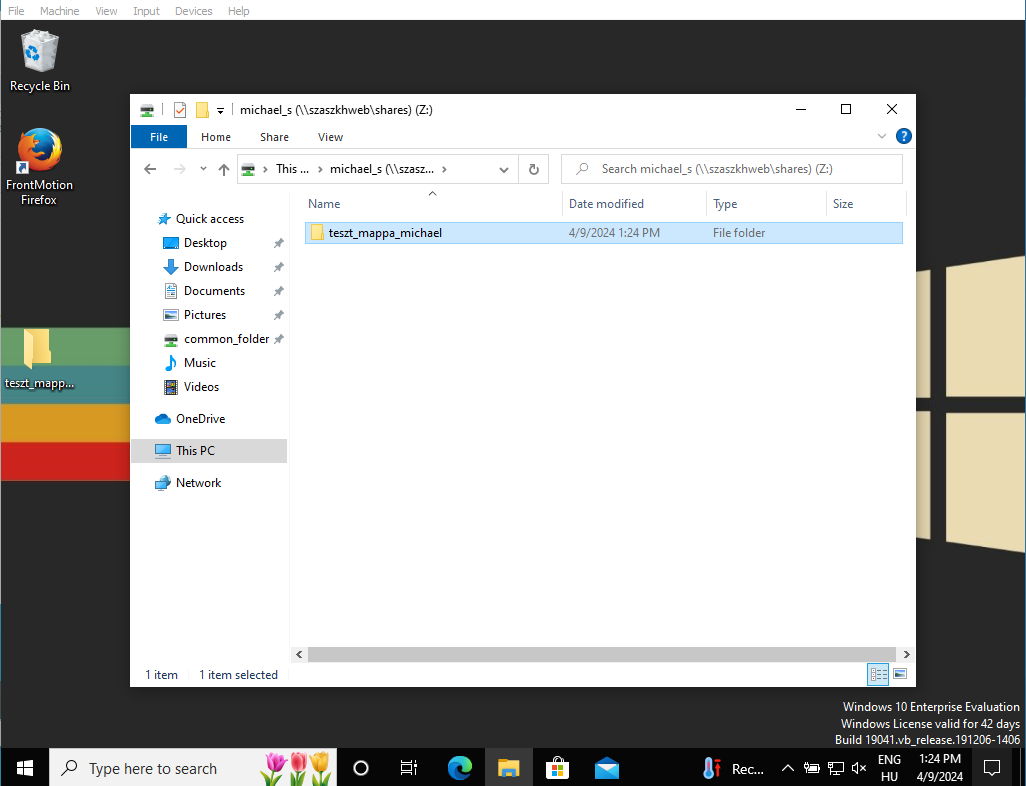


Ha a felhasználó megpróbálja megnyitni ezeket az alkalmazásokat, egy üzenetet kap, melyen az áll, hogy funkció, melyet próbál elérni, le van tilva a számára. Ilyen funkciók a Parancssor, a Beállításszerkesztő (Regedit), az Msconfig (Rendszerkonfiguráció), illetve a Vezérlőpult elérése.

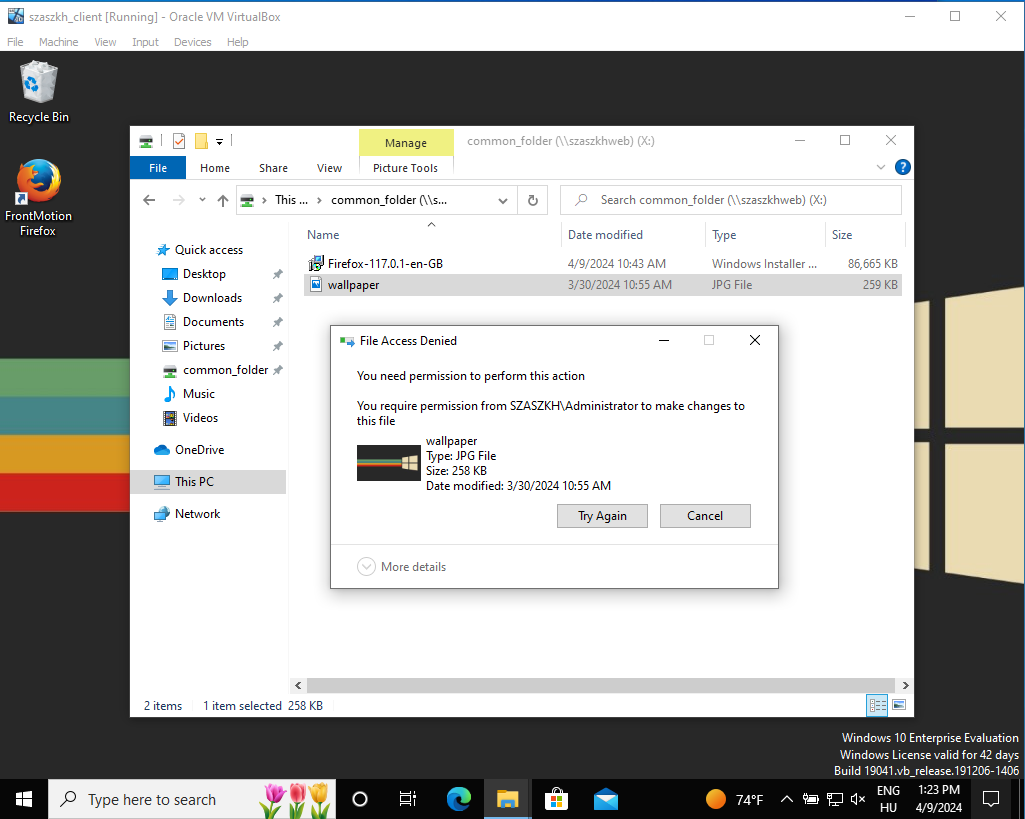
Az adatszivárgás elkerülése érdekében a külső meghajtók (pendrive, külső SSD) csatlakoztatása nem engedélyezett. Az alkalmazottaknak tilos eltárolni a páciensek bizalmas adatait. Ezen adatok csakis a kórház által biztosított számítógépeken/adatbázisban kerülhetnek megőrzésre.



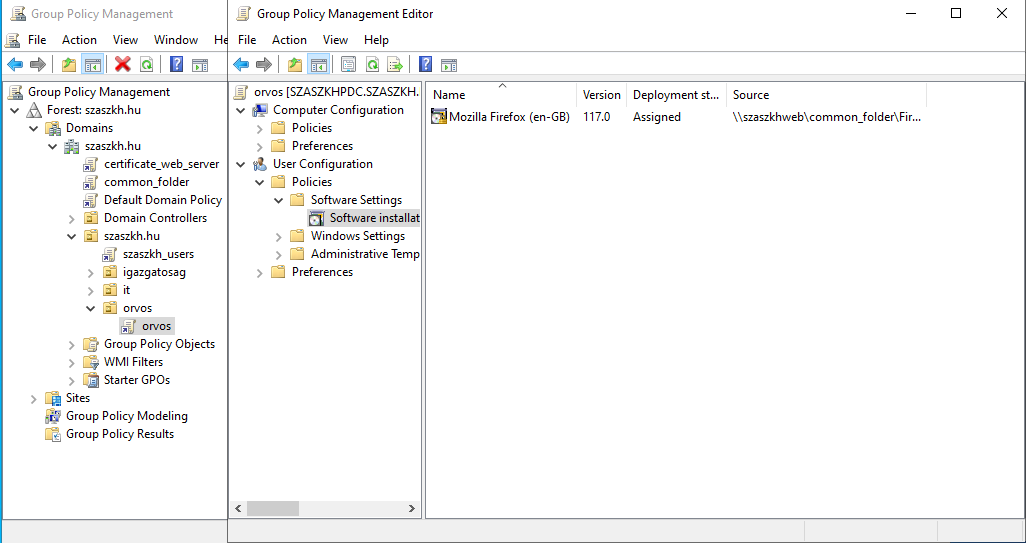
Habár a felcsatlakoztatott Pendrive-ot megjeleníti számítógép, a felhasználó nem fér hozzá a rajta megtalálható fájlokhoz és nem képes adatokat rátenni sem.

 Arra a célra, hogy a felhasználó megőrizhesse saját dokumentumait/fájljait, a Webszerver minden dolgozónak biztosít, egy saját névvel ellátott 500 Megabájtos mappát. Ebből a mappából bármit törölhet, hozzáadhat annyi fájlt, ameddig meg nem haladja a megadott tárhelymennyiséget.

ábra 11 - Dolgozó saját mappája

A képen látható „common\_folder” szintén egy megosztott mappa mely csak olvasható a dolgozók számára. Az oka, hogy ez a mappa csak olvasható az, hogy ebben a mappában találhatóak meg azon alkalmazások, melyek Automatikusan telepítésre kerülnek a felhasználó számítógépére.

Ahogyan a képen is látható, a felhasználótól megtagadja a rendszer a hozzáférést, így nem tud törölni és hozzáadni. Ez azért szükséges, ugyanis az automatizált szoftvertelepítéshez szükséges .msi kiterjesztésű fájlok itt kerülnek eltárolásra.

A fentebb már említett Automatizált Szoftvertelepítés szintén egy csoportházirendnek köszönhető. A csoportházirendet azon szervezeti egyégekhez kell hozzárendelni, amely szervezeti egység felhasználóinak számítógépén szeretnénk automatizált szoftvertelepítést megvalósítani.

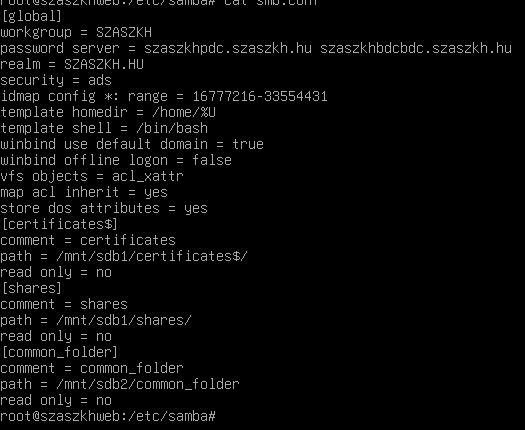
Ahogyan a képen látható, az Orvosok szervezeti egysége alatt található egy csoportházirend, melybe belépve, A szoftvertelepítés fülön belül, egy böngészőt telepítünk. Szoftverek széles választéka megtalálható az Interneten ilyen formában. Fontos, hogy csakis megbízható forrásból telepítsünk ilyen alkalmazásokat. Ezen alkalmazások automatikusan települnek a felhasználók számítógépére minden bejelentkezés után.



ábra 12 - Automatizált Szoftver Telepítés

Mint a képen látható, bejelentkezés után a „Firefox” böngésző megjelent a felhasználó asztalán.

A Linux szerver a Samba nevű Domain Controller segítségével lett hozzárendelve a SZASZKH domainhez, ezen felül a Samba config fájljában lett elvégezve a megosztott mappák konfigurálása.



ábra 13 - Samba - smb.conf

,

### Tanúsítvány

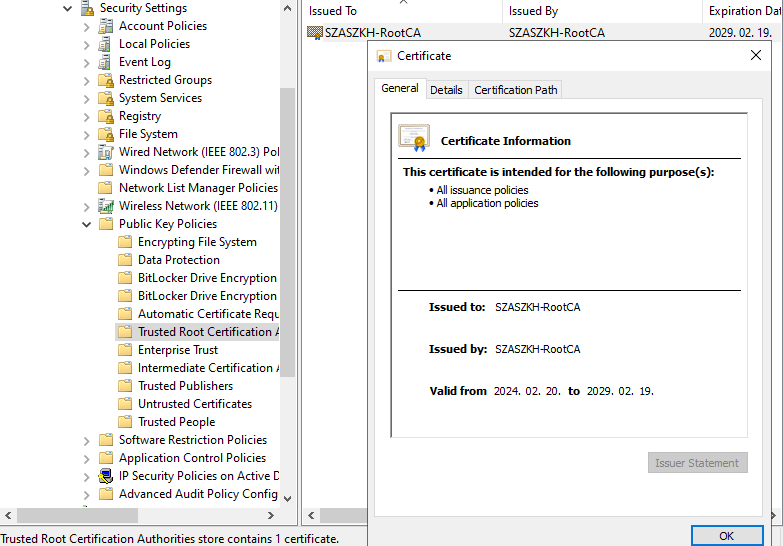
Fontos, hogy a kórház weboldalát látogató személyek adatai biztonságban legyenek. Ehhez, egy tanúsítványozott weboldal megléte szükséges, mely titkosított (HTTPS) forgalmat biztosít.

Az OpenSSL segítségével létrehozott tanúsítvány a Linux Webszerveren található.

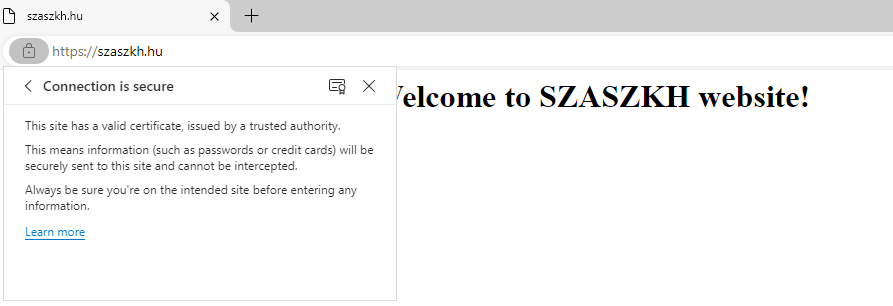
ábra 14 - Weboldal tanúsítvány

A képen látható hosszú karakterlánc, a CA privát kulcsa, mely sha256 titkosítással rendelkezik.

Ezen kulcspár létrehozása önmagában még nem elég.

A tanúsítványt a PDC szerveren fel kell vennünk egy csoportházirendbe, mely kimondja, hogy a tanúsítvány megbízható.

ábra 15 - Megbízható tanúsítvány

Ennek eredménye, hogy a megnyitott „**szaszkh.hu**” csakis HTTPS protokollt használ, és aktív tanúsítvánnyal rendelkezik.

ábra 16 - Aktív tanúsítvánnyal rendelkező weboldal

Backup.sh script