Gradus Vol 2, No 2 (2015) 104-111
ISSN 2064-8014

CSOMAGSZŰRÉS CISCO ROUTEREKEN ACL-EK SEGÍTSÉGÉVEL

PACKET FILTERING ON CISCO ROUTERS USING ACLS

Agg P[1], Göcs L.[1], Johanyák Zs. Cs.[1], Borza Z.[2]*

[1]Informatika Tanszék, Gépipari és Automatizálási Műszaki Főiskolai Kar, Kecskeméti Főiskola, Magyarország
[2]Katedra Gimnázium, Informatikai és Művészeti Szakközépiskola és Kollégium, Magyarország

Kulcsszavak:
hálózatbiztonság
tűzfal
ACL
Packet Tracer

Keywords:
network security
firewall
ACL
Packet Tracer

Cikktörténet:
Beérkezett 2015. november 1.
Átdolgozva 2015. november 10.
Elfogadva 2015. november 10.

Összefoglalás

A számítógépes hálózatok biztonságára különös hangsúlyt kell fektetni a rendszermenedzsment során. Figyelni kell a biztonságos adatáramlásra mind a kimenő, mind a bemenő forgalom esetében. Ebben hatékony segítséget nyújthatnak a forgalomirányítóknál alkalmazott Access Control List-ek (ACL). A cikk célja az, hogy ismertesse az ACL-ek beállítását routereken úgy, hogy azok hatékony védelmet nyújtsanak a belső és külső támadásokkal szemben. A konfigurálást Packet Tracer program segítségével szimulált hálózaton mutatjuk be.

Abstract

The security of computer networks is a prioritized task for network administrators. Secure data flow should be ensured both in case of incoming and outgoing traffics. Access Control Lists (ACLs) could represent a very useful tool for this purpose. This paper describes how ACLs on routers should be configured in order to ensure efficient protection against internal and external attacks. The suggested configuration is tested in a network simulated by Packet Tracer.

1. Bevezetés

Napjainkban gyakorlatilag életünk minden területén találkozunk számítógépes hálózatokkal. Hálózatokon keresztül tartjuk a kapcsolatot barátainkkal, fizetjük számláinkat, rendelünk termékeket, továbbítjuk munkánk bizonyos részeit. Mivel bizalmas, titkos adatok sorát küldjük a hálózatokon keresztül, elengedhetetlen a megfelelő védelem, biztonság.

Biztonság szempontjából a hálózatok esetében nem elegendő, hogy a rendszer jó, működőképes állapotban legyen és folyamatosan abban is maradjon, hanem meg kell gátolni, hogy bizalmas információk a hálózaton kívülre kerüljenek, illetve, hogy illetéktelenek kívülről ne férjenek belső információkhoz. Ahhoz, hogy a megfelelő biztonsági szintet elérjük, szükségünk van arra, hogy a kockázatokat felmérjük, a lehetséges veszélyeket beazonítsuk. Ezt a tevékenységet kockázatelemzésnek nevezzük, és segítségével elérhetjük, hogy hálózatunk gyenge pontjait felderítsük, és megfelelően biztosítsuk.

Biztosan elmondható, hogy tökéletesen biztonságos hálózat nem létezik, csak törekedhetünk arra, hogy minél kevesebb legyen a gyenge pont. Kísérletet kell tenni arra, hogy az úgynevezett „leggyengébb láncszemet”, azaz a felhasználót, minél jobban tehermentesítsük, biztosítsuk. A

* Kapcsolattartó szerző. Tel.: +36 76 516 418; fax: +36 76 516 399
E-mail cím: agg.peter@gamf.kefo.hu

hálózatok biztonságos hozzáférését több féle módszer segítségével is elérhetjük. Alapvető elvárás a hálózatok biztonságával szemben a felhasználó azonosítása (autentikáció), ami lehet gyenge azonosítás (felhasználói név, jelszó) vagy erős azonosítás (kétfaktoros, háromfaktoros azonosítás). Ehhez elengedhetetlenül szükséges egy hálózati házirend, ami tartalmazza a jelszavakkal szembeni elvárásokat (pl. kis- és nagybetű, szám, lejárati idő). Ezen felül szükség van titkosításra, tartalombiztonságra. Vezeték nélküli hálózatoknál ezt napjainkban a WPA2-es titkosítással oldják meg [4], illetve az SSID tiltásával. Nagyon fontos szerepet játszanak a hálózatvédelemben a tűzfalak. A tűzfalak két hálózat között helyezkednek el, és feladatuk, hogy a rajtuk áthaladó forgalmat szabályozzák a megfelelő előírások, biztonsági szempontok (policy) alapján. Általában a nyilvános és a magánhálózatok közé helyezik el a tűzfalakat. Legtöbbször többszintű védelemmel látják el a magánhálózatokat, és szükség esetén használnak egy úgynevezett DMZ-t (DeMilitarizált Zóna: szigorúan védett privát hálózat és a nyilvános hálózat közé beépített közbülső védelem) is [5]. A hálózatokat és a DMZ-t egy vagy több tűzfalas megoldásokkal határolhatják el. A tűzfalak legegyszerűbb változata a csomagszűrő tűzfal, amit a CISCO routereknél a hozzáférés vezérlő listák (ACL) segítségével oldhatunk meg.

Cikkünkben ezen hozzáférési listák használatát és beállításait ismertetjük. Szimulált hálózaton mutatjuk be az ACL beállításainak lépésit, majd a megvalósulás után a tesztelést. A szimulációhoz a CISCO Packet Tracer programot használjuk. Célunk annak bemutatása, hogy a hozzáférési listákkal könnyen tudunk megvalósítani biztonságos csomagforgalmat, mellyel a hálózat működésének hatékonyságát is biztosítjuk.

2. Hozzáférés-vezérlési listák

Az Access Control List (ACL), azaz hozzáférés-vezérlési lista a forgalomszűrés egyik legelterjedtebb változata [2]. Az ACL-ek segítségével hozzáférés vezérlést biztosítunk egy erőforráshoz. Segítségükkel ellenőrizhetjük a hálózatba bejövő illetve kimenő forgalmat, és szükség esetén még szűrhetjük is azt. A forgalomszűrés javítja a hálózat teljesítményét.

Az ACL segítségével az elosztási rétegben korlátozható a hozzáférés, és megakadályozható a nem kívánt forgalom központi hálózatba jutása. A hozzáférési listával ellenőrizhető a forgalomirányító interfészein áthaladó hálózati forgalom. Ez azt jelenti, hogy az OSI modell 3. rétegében dolgozunk, vagyis megelőzzük jóval a szoftveres védelmet. Az ACL-ek engedélyezhetnek és tilthatnak is forgalmat a megfelelő szabályokkal. Az ACL-ek megadási sorrendben hajtódnak végre, a szoftver végigmegy szabályokon, és amelyik megfelelő neki, azt végrehajtja. Ha nincs a kérésre vonatkozó meghatározás, az egyéb beállítások lépnek érvénybe. Háromféle ACL típus különböztethetünk meg, ezek a normál, a kiterjesztett és a nevesített ACL [2].

Normál ACL

A normál ACL (Standard ACL) a legegyszerűbb a három típusból. Forrás IP-cím alapján végzi a szűrést, teljes protokollműködés alapján tiltja vagy engedélyezi a forgalmat. Ha egy ilyen ACL nem engedélyezi egy munkaállomás IP forgalmát, az erről az állomásról érkező összes szolgáltatást letiltja. Lehetőségünk van egy adott felhasználó vagy helyi hálózat számára engedélyezni az összes szolgáltatás elérését a forgalomirányítón keresztül, míg az összes többi IP-cím esetén tilthatjuk a hozzáférést. A normál ACL-ek a hozzájuk rendelt azonosítási szám alapján azonosíthatók be. Az azonosítási számnak 1 és 99, illetve 1300 és 1999 közé kell esnie. Pl. a *Router(config)#access list 2 permit host 172.16.1.80;* ACL a 172.16.1.80 IP címet engedélyezi.

Kiterjesztett ACL

A kiterjesztett ACL (Extended ACL) már nem csupán a forrás IP-cím alapján, hanem a cél IP-cím, a protokoll és a portszámok segítségével is szűrhet. Sokkal elterjedtebb, mint a normál ACL, mivel jobb ellenőrzést tesz lehetővé, és specifikusabb is. Azonosítási számuknak 100 és 199, illetve 2000 és 2699 közé kell esniük. Pl. a *Router(config)#access list 102 permit 192.168.2.0 0.0.0.255 any;* ACL a 192.168.2.0 hálózat minden állomását engedélyezi, ugyanakkor minden mást tilt. Továbbá a *Router(config)#access-list 103 deny tcp any 192.168.2.0 0.0.0.255 range 20 2;* a teljes FTP forgalmat letiltja. A *Router(config)#access-list 101 deny tcp 195.220.0.0 0.0.255.255*

0.0.0.0 0.0.0.0 eq 80; ACL-lel tiltjuk a 195.220.0.0/16 hálózat felől a HTTP (80-as port) kéréseket bármilyen célhálózat felé.

Az ACL definiálását egy interfészhez történő hozzárendelés követi 1

(config)#interface Serial 0
(config-if)#ip access-group 1 out (kimenő interfész)
(config)#interface Ethernet 0
(config-if)#ip access-group 101 in (bejövő interfész)

Nevesített ACL

A nevesített ACL (Named ACL, NACL): normál vagy kiterjesztett hozzáférési lista, ahol az azonosító szám helyett egy névvel hivatkozunk a listára. A nevesített ACL-ek beállításához a forgalomirányítón NACL üzemmódban kell lennünk.

Az ACL-ek végén mindig van egy implicit tiltás, tehát mindent tiltunk alapesetben, azon kívül, amit engedélyeztünk. Ez a gyakorlatban azért bevett szokás, mert ilyenkor nem a tiltásokat, hanem az engedélyeket vesszük sorra, amit a szükséges ACL-ekkel tudunk megadni. Ebben az esetben nem fordulhat elő az eset, hogy a biztonsági tervezés alatt elfelejtenénk bármely biztonsági szempontból fontos elem tiltását!

Ha a nemkívánatos forgalomforráshoz közel tiltunk, akkor a forgalom nem halad keresztül az egész hálózaton, és foglal le értékes erőforrásokat. A hozzáférési listák minden olyan forgalmat ellenőriznek az ACL-ben megadott szabályoknak megfelelően, amelyek áthaladnak az eszköz megadott interfészén. Az ACL-ek helytelen használatából előfordulható hibák az alábbi típusúak lehetnek.

- Az összes csomag ellenőrzése jelentősen leterheli a forgalomirányítót, így kevesebb időt tud fordítani a csomagtovábbításra. Ilyenkor használható a sorba állítás, amikor protokollok szerint a router egyes csomagokat előbbre vesz, és egyes csomagokat, amelyek nem fontosak, fel sem dolgoz.
- A rosszul megtervezett ACL-ek sokkal nagyobb terhelést okoznak, ami a hálózat működésében zavart, hibát okozhat.
- A nem megfelelően elhelyezett ACL-ekkel pont az ellenkezőjét érhetjük el, mint amit szerettünk volna. Blokkolhatjuk az engedélyezni kívánt, és engedélyezhetjük a tiltani kívánt forgalmat [9].

A jól megtervezett hozzáférési listákkal csökkenthetjük a hálózat terhelését, és jóval kisebb sávszélességet használunk fel.

3. Konkrét megvalósított példa Cisco Packet Tracerben

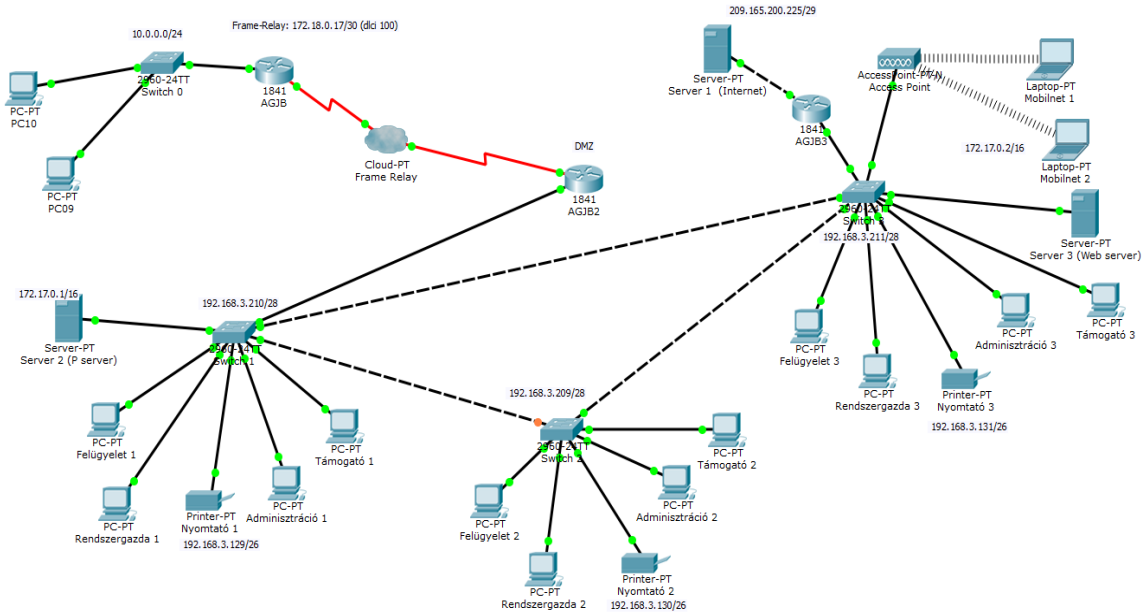
Az alábbiakban röviden bemutatjuk a szimulációhoz használt Cisco Packet Tracer programot. A Cisco Packet Tracer egy emulációs program, amiben könnyen megtervezhetjük, létrehozhatjuk, és tesztelhetjük a kigondolt hálózati konfigurációt. A programban megjelenő eszközöket konzolosan vagy varázsló segítségével állíthatjuk be. Számos forgalomirányítót, kapcsolót, vezeték nélküli eszköz és végberendezést tartalmaz a program, ezeket a megfelelő beállítások után a valóságnak megfelelően működtethetjük.

Konkrét példánkban egy kitalált cég hálózatát hoztuk létre, melynek feladataihoz a tartozik többek között hivatalos esemény rögzítése, megosztása élőben, illetve későbbi időpontban ezek webkiszolgálóról történő megtekintése. Ezen kívül a cég munkatársai felügyelik a szervereken tárolt videó anyagokat, és esetleges probléma esetén támogatást nyújtanak.

Egy többszintű-, hierarchikus címzési- és elnevezési sémában kellett gondolkodnunk, amivel megoldható, hogy a későbbiekben a hálózathoz esetleg újonnan hozzáadott felhasználók, illetve eszközök egyszerűen és könnyen felügyelhetők legyenek. Meg kellett oldani továbbá a külvilág felé megosztott tartalmakat (például a rögzített tárgyalási események) tároló eszközök egy, a belső hálózattól szigorúan szabályozott módon elkülönített, úgynevezett *demilitarizált zóná*ba (*DMZ*) történő elhelyezését. Ezzel a megoldással értük el azt, hogy a kívülről érkező támadások egy, a biztonsági szempontból érzékeny területtől jól elválasztott alhálózatba érkezzenek. A létrehozott belső címzési séma külvilágtól történő elrejtésére a Network Address Translations-t (NAT-ot), azaz

a *hálózati címfordítást* alkalmaztuk. Segítségével a cég belső privát címei egy és ugyanazon publikus, mások által is látható címre történő lefordításával megakadályoztuk, hogy kívülről „felderíthető” legyen a hálózat struktúrája. A külső támadások mellett a belső forgalom szűrése is szükséges, így kiszűrhető az egyes hálózati területekre bejövő, illetve onnan származó nem megengedett csomagforgalom. Így a felesleges forgalom kiszűrésével a hálózat sávszélessége is javítható. Minden hálózati eszköz távolról történő elérését úgy kell biztosítani, hogy a megfelelő erősségű jelszavakkal védhetők legyenek a jogosulatlan hozzáférések elől.

A fenti szempontokat és tervezési megfontolásokat figyelembe véve, az alábbi szimulált hálózatot hoztuk létre.



1. ábra. A megvalósított hálózat

Biztonságpolitikai követelmény volt, hogy távoli helyszínekről, ideértve a külső irodákat is, csak bizonyos helyi hálózati erőforrásokat legyenek elérhetőek. A szükséges szabályok a következők.

interface Serial0/0/0 (erre a portra állítjuk be)
description Frame-Relay kapcsolat
ip address 172.18.0.18 255.255.255.252
encapsulation frame-relay (beágyazás)
frame-relay interface-dlci 200 (beállítás a kapcsolathoz)
ip access-group 101 in (bejövő)
ip access-group 102 out (kimenő)

A távoli felhasználóknak (PC09, PC10) hozzá kell férni a P Serverhez, hogy láthassák a tartalmukat a weben keresztül,

access-list 101 permit tcp host 172.18.0.17 host 172.17.0.1 eq www

A távoli felhasználóknak képesnek kell lenni a P Serverekről fájlokat letölteni illetve oda feltölteni FTP segítségével.

access-list 101 permit tcp host 172.18.0.17 host 172.17.0.1 range 20 21 ftp

A távoli felhasználók használhatják a P Servert, hogy e-mailt küldjenek és fogadjanak SMTP és IMAP protokollok segítségével.

access-list 101 permit tcp host 172.18.0.17 host 172.17.0.1 eq smtp
access-list 101 permit tcp host 172.18.0.17 host 172.17.0.1 eq 143

A távoli felhasználók nem érhetnek el semmilyen más szolgáltatást a P Serveren. Megjegyzés: Az ACL-ek végén mindig van egy implicit tiltás, vagyis az engedélyezetten kívül minden tiltva van.

access-list 101 permit tcp any any implicit tiltás

Nem engedélyezett a központi iroda munkaállomásairól a távoli felhasználók munkaállomásai felé tartó forgalom. Minden olyan fájlt, amit a két helyszín között szükséges átvinni, a P Serveren kell tárolni, és onnan lehet őket FTP segítségével elérni (vissza irány engedélyezése).

access-list 102 permit tcp any any

Nem engedélyezett a távoli helyszín munkaállomásairól a központi helyszín munkaállomásai felé tartó forgalom.

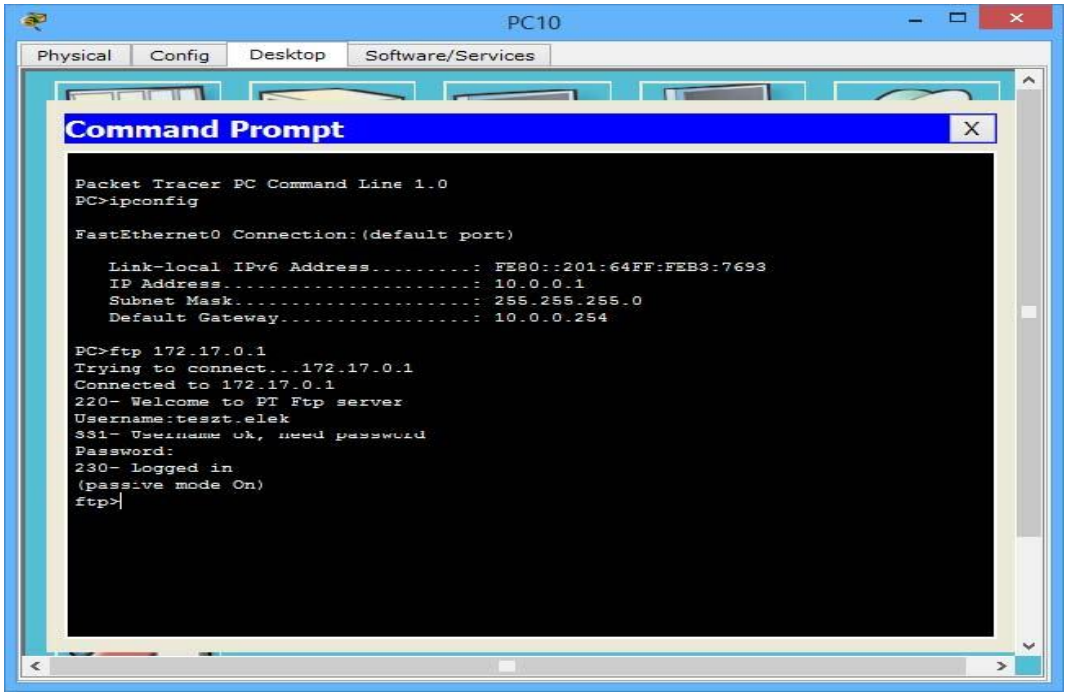
access-list 102 deny ip 192.168.0.0 0.0.3.255 10.0.0.0 0.0.0.255

A központi irodában lévő routereket és switcheket csak a 70-es vlan munkatársai érhetik el Telnet segítségével.

line vty 0 4
access-class 70 in
password 7 0822455D0A16
login

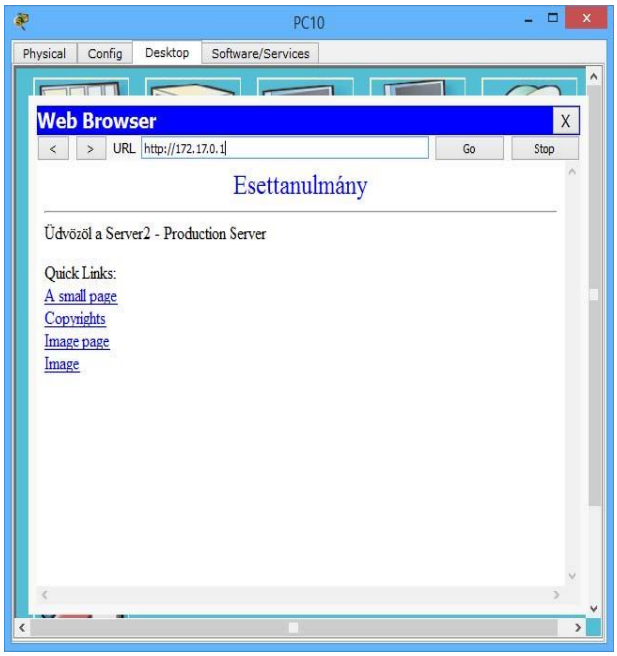
4. Az ACL beállítások tesztelése

Az alábbi tesztkimeneten látható, hogy a PC10-es távoli felhasználó az FTP protokollon keresztül éri el a P Servert. (2. ábra)

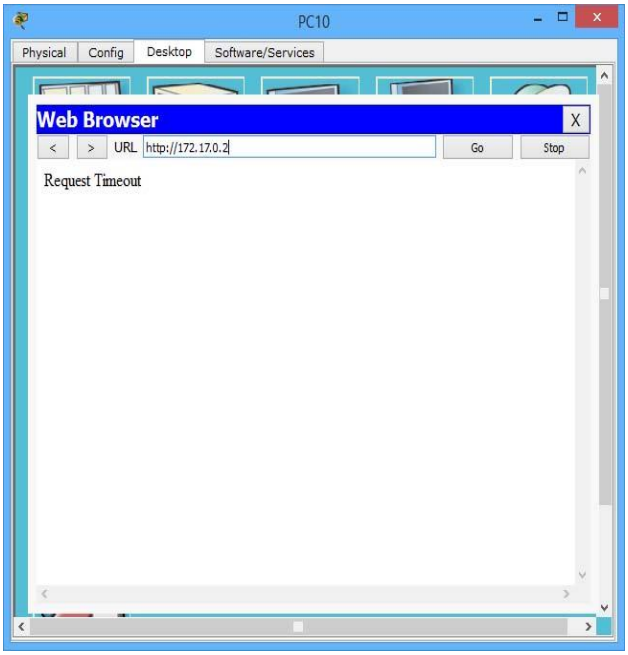


2. ábra. Teszt eredménye

A következő két teszteredmény azt mutatja, hogy a távoli felhasználó HTTP protokollon keresztül éri el a P Server-t (3. ábra), illetve azt, hogy nem sikerül elérniük a Server 3-at (172.17.0.2) (4. ábra).

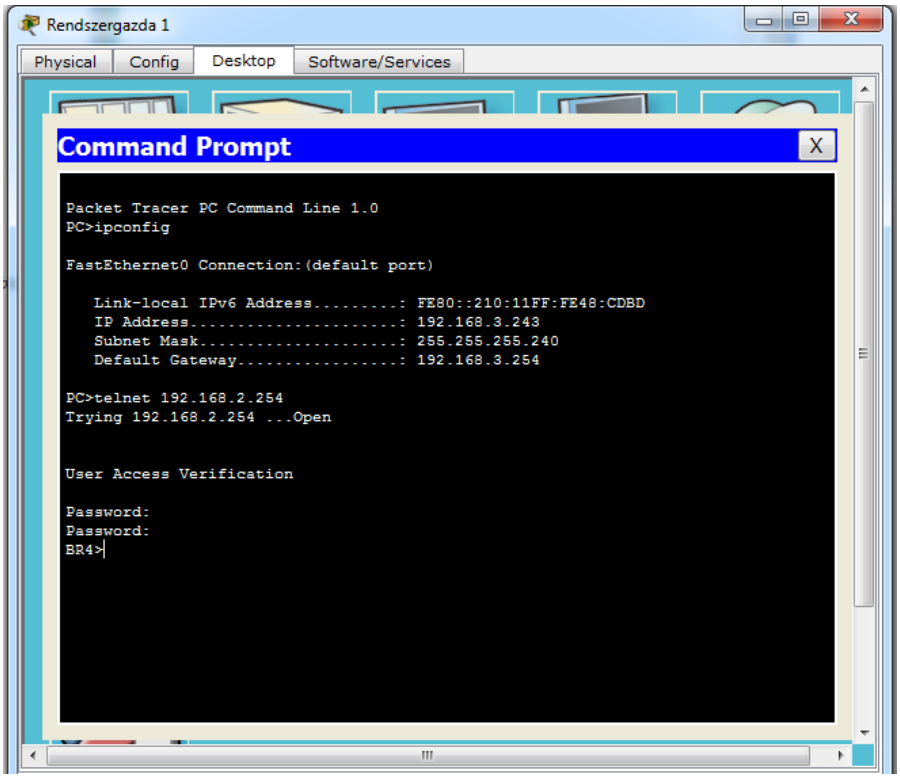


3.ábra. HTTP teszt sikeres



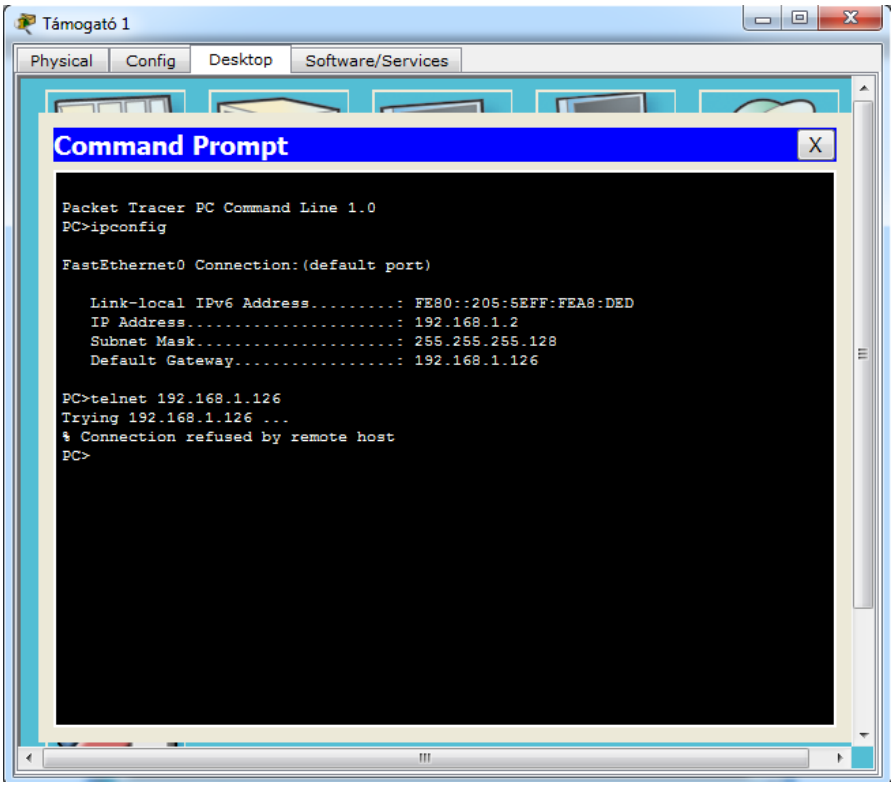
4.ábra. HTTP teszt sikertelen

A 70-es VLAN-ba (Pl: Rendszergazda 1) tartozó felhasználók elérik a hálózati eszközöket (5. ábra)



5. ábra. A teszt eredménye

Azon felhasználók, akik nem a 70-es VLAN-ba tartozó (Pl: Támogató 1) gépen dolgoznak, nem érik el telnet segítségével a hálózati eszközöket (6. ábra).



5. ábra. Teszt eredménye

5. Következtetések

A cikkben bemutattuk, hogy az ACL-kel nagyon egyszerűen és hatékonyan lehet szabályozni a hálózati forgalmat. Elsősorban a távoli használatra mutattunk be példákat, de természetesen ezt lehet bővíteni helyi hálózaton belül. Fontos, hogy a jól megtervezett, jól elhelyezett ACL-ek, nem csak biztonságosabb hálózatot biztosítanak, hanem elősegítik a hálózat jobb kihasználását, hatékonyabb működését is.

Irodalomjegyzék

[1] Cisco 2900 Series Integrated Services Routers Data Sheet http://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.pdf
[2] CCNA Discovery 3: Introducing Routing and Switching in the Enterprise 8. fejezet
[3] CCNA Discovery 4: Designing and Supporting Computer Networks. 1-9. fejezet
[4] Hogyan tegyük biztonságossá a Wi-Fi hálózatot http://pcworld.hu/hardver/hogyan-tegyuk-biztonsagossa-a-wi-fi-halozatot.html
[5] DMZ hálózatok tervezése és használata, Linuxvilág, 2001 május, http://linuxvilag.pbk.hu/content/files/cikk/06/cikk_06_40_44.pdf