**Vizsgaremek - Corp vállalat informatikai rendszere**

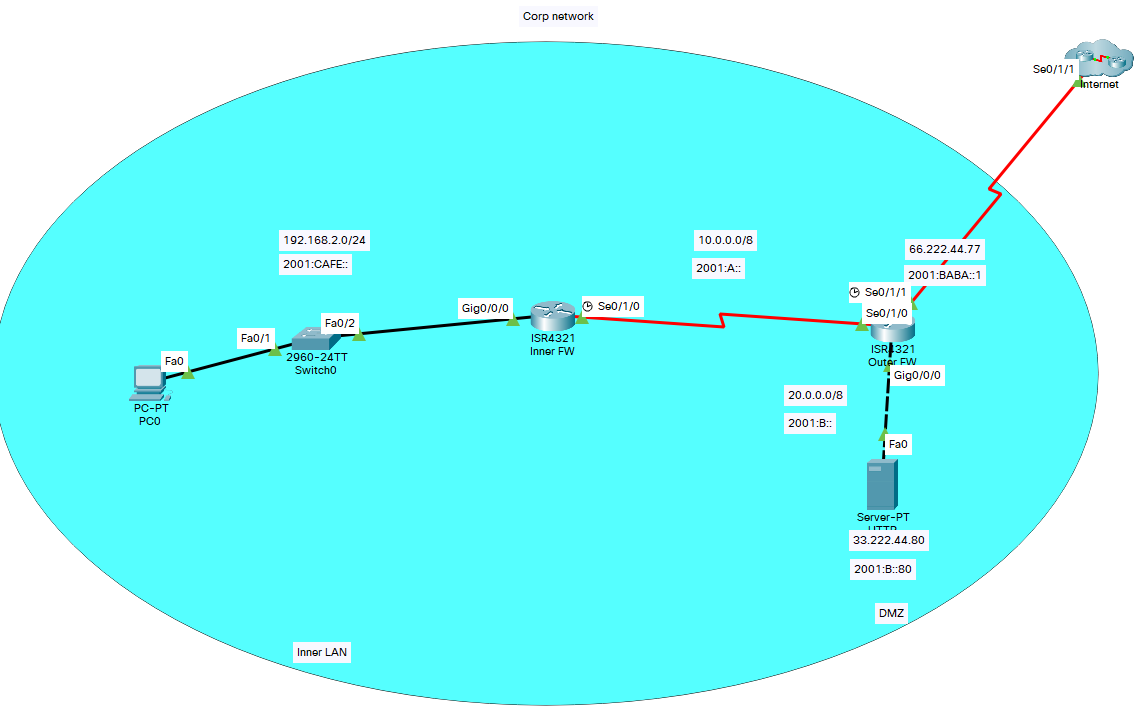
**XXX**

**A feladat leírása:** Corp vállalat megbízott a már meglevő informatikai hálózatának kibővítésével. A feladat, hogy beállítsunk egy HTTP kiszolgálót, melyet a belső hálózatról, és az internet felől is el lehet érni. A megvalósítás legyen ésszerű, gyors, költséghatékony és biztonságos. A hatékonyság érdekében szabad kezet kaptunk, teljesen át lehet (és kell) tervezni a hálózatot.

Rendelkezésre álló erőforrások:

* *ISR4321 router 2 db*
* *2960-24TT switch*
* *PC win 10-zel 10-12 db*
* *soros vonali internetkapcsolat, ISP: 66.222.44.78/8, 2001:BABA::2/64*
* *külső DNS kiszolgáló: 192.168.1.2/24, 2001:FFFF::2/64*

A feladathoz tartozó fájlok: DMZ.pkt, HTTP.vdi (teszt prototípusokat segítő részletek)

1. ábra: Topológia PT-ből

**A vizsgaremek követelményei közül megvalósított pontok:**

* IPv4 és IPv6 címzési rendszert egyaránt használ
* forgalomirányítón megvalósított biztonsági funkciókat tartalmaz (pl. ACL-ek)
* statikus forgalomirányítást egyaránt megvalósít
* statikus címfordítást alkalmaz
* Linux kiszolgálót tartalmaz
* HTTP/HTTPS
* a hálózat tervét, működésének leírását tartalmazó dokumentáció
* a hálózat tesztelésének dokumentációja
* Linux kiszolgálót tartalmaz
* HTTP

A dokumentációt az áttekinthetőség érdeklben TCP/IP modell szerinti csoportokra osztottuk, melyek egyenként tartalmazzák az adott csoport követelményeit, megvalósítását és tesztelését.

A munka során elkészítettük az egyes részfeladatok szimulációit, melyeket lehetőség szerint integrálva próbáltuk a teljes hálózatot tesztelni. Ezekre alapozva fizikai eszközökön is felépítettünk egy működő prototípust. A kettő közötti eltérések leküzdése miatt nem kellett jelentős változtatásokat eszközölni. A HTTP kiszolgálót az egyik rendelkezésre álló PC-re telepítettük, Linuxot használva. A továbbiakban a leírás kizárólag a működő prototípusra vonatkozik!

**Hálózatelérési réteg**

**követelmény:**

**megvalósítás:**

**tesztelés:**

**Internet réteg** (csak routing)

**routing követelmény:**

Dual stack-et kellett megvalósítani. A hálózat bővíthetősége nem volt fő szempont. A gyors és hatékony működésen van a hangsúly.

**routing megvalósítás:**

IPv4 esetén a NAT-ot figyelembe véve adtuk meg az útvonalakat. IPv6-nál a globális címek közvetlenül vannak felhasználva a forgalomirányításhoz. A kapcsolódó hálózatok nem igényelnek külön beállítást. Inner-nél mivel csak egy útvonal jöhet szóba, alapértelmezett útvonalat használtunk az internetelérés miatt. Outernél internet felé szintén alapértelmezett útvonalat használtunk, de itt már a LAN felé is meg kellett adni az útvonalat.

**routing tesztelés:**

A végső teszteket a HTTP elérésével végeztük. Ping az ACL-ek miatt nem működik. Itt nagy segítség volt a PT környezete, ahol követni tudtuk a csomagokat. A LAN-ból indulva a DNS az alapértelmezések szerint az internetre ment, és vissza is talált a végponthoz. A megszerzett IP alapján a legrövidebb úton megtalálta a HTTP-t, mivel Outeren ez kapcsolódó hálózat (NAT!). Internet felől gond nélkül elérhető a DMZ, a belső hálózatot nem érinti a forgalom. A prototípuson az elvárt sebesség és megbízhatóság mellet működik az elérés bármely végpontról.

**Szállítási réteg**

**követelmény:**

**megvalósítás:**

**tesztelés:**

**Alkalmazási réteg**

**HTTP kiszolgáló – Linux**

Készítette: Babusa Tamás

**követelmény:**

Debian 10 LTS

user: x, pass: y

IP: 192.168.0.37

A vállalatunk HTTP szolgáltatását Linux kiszolgálóra telepítettem. Kiszolgálónak egy virtuális számítógépet használtam, Debian 10 LTS operációs rendszerrel. A szolgáltatáson kívül több egyéb alkalmazás is beállításra került, ami elsősorban a biztonságot és kismértékben a kényelmet szolgálja. Az így felépített webszerver a helyi hálózat és az internet felől is elérhető. A külső elérést a határ routeren beállított port forwarding biztosítja. Ezen kívül az SSH is működik külső hálózatból, szintén Ford port forwarding segítségével.

**megvalósítás:**

Hardening:

Az összes módosított konfigurációs fájlról másolatot készítettem, így sokkal könnyebbé válik az esetleges visszaállítás.

A root felhasználót letiltottam biztonsági okokból. Helyette egy sudoer felhasználóval lehet dolgozni. Az SSH beállításánál egy biztonságos hosszúságú SHA kulcsot használok. Password helyett passphrase-t használok. Jelszóval nem lehetséges bejelentkezni. Root felhasználóval sem lehet be SSH-zni. Továbbá letiltottam az IPv6-os címeket. Az alapértelmezett 22-es portját 2222 lecseréltem (lsd. függelék).

A kissé nehézkes IP tables tűzfal alkalmazást töröltem, helyette NF tables-t használok. Alapvető filozófiám volt, hogy csak és kizárólag azt engedem át a tűzfalon, ami a minimális működéshez szükséges. Az illegális csomagokat automatikusan kiszűri és a megfelelő .log fájlba elkönyveli ennek tényét (/log/xy.log). Fogadja az SSH, HTTP és a z ICMP csomagokat, minden más próbálkozást megszámol és logol. A forwarding tiltva van és a kifelé irányuló adatforgalom teljes egészében engedélyezett (lsd. függelék).

Szolgáltatások:

A HTTP szolgáltatáson kívül egy NTP-t is telepítettem az online időszinkronizálás miatt. HTTP-nek az Apache2-t választottam. Praktikus okokból a nyolcvanas, alapértelmezett portot hagytam meg a weblap eléréséhez. A weblap elérére a www-Data user jogosult, ezért ennek elérési jogait korlátoztam olvasásra és végrehajtásra a weblap mappájában. Az alapértelmezett WWW mappát letiltottam. Ezzel a weblap illetéktelenek számára nem módosíthatóvá vált. mivel a weblapunk statikus, erre nincs is szükség (lsd. függelék).

**tesztelés:**

A tesztelést két részre bontottam; először a hardeninget, utána magát a HTTP szolgáltatást teszteltem.

A hardening tesztelésénél megpróbáltam be SSH-zni mind helyi, mind távoli hálózatról. Root felhasználóval nem jártam sikerrel. A jelszó használata nem megengedett. Nem lehet bejelentkezni IPv6-os címen sem, mivel nincs ilyen. Nem elérhető a szerver, ha SSH-nál Nem adjuk meg ha 2222-es portot. Az alapértelmezett 22-es szintén nem elérhető (ssh –p2222 x@ip).

A szerver megfelelő .log fájljait átnézve találtam riasztásokat (/log/xy.log).

Próbaképpen letiltottam az ICMP, SSH és a http protokollokt és megpróbáltam elérni ezeket a szolgáltatásokat. Ezek természetesen tiltott állapotban nem működtek. Ezt követően a szerverről próbáltam megpingelni különböző helyi és távoli hálózatok hosztjait. Ezek az elvárásoknak megfelelően működtek. A HTTP szolgáltatás bármely hálózatban működött, visszaadta a feltöltött weblapunkat.

A Debian szerver működőképes, megfelelően konfigurált a projekt többi részéhez, és kellő védelemmel van felvértezve, így el tudja látni a delegált funkciókat.

**Bővítési lehetőségek**

Egy belső DNS használata megfontolandó, ugyanis a LAN-ból induló kérések kimennek az internetre, ami jelentős lassulást eredményezhet, esetleg teljes működésképtelenséget, ha a szolgáltató nem működik. Ehhez egy másik (virtuális) szervert javaslunk, a jobb terheléselosztás érdekében.

…

A szerver átkerülhet virtuális térbe, amennyiben több olyan szolgáltatásra is igény lesz, amiket előnyös különválasztani. Egy lightweight Linux distribution alatt több szerver is gond nélkül működhetne, terheléstől függően. Ez esetben a lemezképek kezelése is jelentősen leegyszerűsödne.

**Források**

…

…

**Függelék**

**Címzési séma:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **eszköznév** | **interfész** | **IP** | **maszk** | **átjáró** |
| PC0 | Realtek-x | 192.168.2.10 | /24 | 192.168.2.1 |
| PC0 | Realtek-x | 2001:CAFE::10 | /64 | FE80::1 |
| Inner-FW | G0/0/0 | 192.168.2.1 | /24 | - |
| Inner-FW | S0/1/0 | 10.0.0.1 | /8 | - |
| Inner-FW | G0/0/0 | 2001:CAFE::1 | /8 | - |
| Inner-FW | S0/1/0 | 2001:A::1 | /8 | - |
| … |  |  |  |  |
| … |  |  |  |  |
| DNS | szolgáltató | 192.168.1.2 | szolgáltató | szolgáltató |
| DNS | szolgáltató | 2001:FFFF::2 | szolgáltató | szolgáltató |

**VLAN:**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **név** | **hálózat** |
| VLAN 1 | **-** | **-** |
|  |  |  |

**Jelszavak:**

|  |  |
| --- | --- |
| **eszköz, felhasználó vagy protokollnév** | **jelszó/kulcs** |
| Inner-FW enable | cisco |
| Inner-FW console | cisco |
| Outer-FW enable | cisco |
| Outer-FW console | cisco |
| … |  |

**Eszközökön használt szkriptek:**

|  |  |  |
| --- | --- | --- |
| **eszköznév** | **szkript** | **megjegyzés** |
| Inner-FW | en  conf t  ipv6 unicast-routing  ip route 0.0.0.0 0.0.0.0 s0/1/0  ipv6 route ::/0 s0/1/0  int s0/1/0  ipv6 enable  ip add 10.0.0.1 255.0.0.0  ipv6 add 2001:A::1/64  no sh  int g0/0/0  ipv6 enable  ip add 192.168.2.1 255.255.255.0  ipv6 add 2001:CAFE::1/64  ipv6 add FE80::1 link-local  no sh  ip access-list extended SURFING  permit tcp 192.168.2.0 0.0.0.255 any eq 80  permit tcp 192.168.2.0 0.0.0.255 any eq 443  permit udp 192.168.2.0 0.0.0.255 any eq 53  permit tcp 192.168.2.0 0.0.0.255 any eq 53  exit  ip access-list extended BROWSING  permit tcp any 192.168.2.0 0.0.0.255 established  permit udp any eq 53 192.168.2.0 0.0.0.255 range 1024 5000  ex  ipv6 access-list SURFINGv6  permit tcp 2001:CAFE::/64 any eq 80  permit tcp 2001:CAFE::/64 any eq 443  permit udp 2001:CAFE::/64 any eq 53  permit tcp 2001:CAFE::/64 any eq 53  exit  ipv6 access-list BROWSINGv6  permit tcp any 2001:CAFE::/64 established  permit udp any eq 53 2001:CAFE::/64 range 1024 5000  int g0/0/0  ip access-group SURFING in  ip access-group BROWSING out  ipv6 traffic-filter SURFINGv6 in  ipv6 traffic-filter BROWSINGv6 out | Dual stack mindenhol következetesen  SLAAC használatra kész |
| Outer-FW | en  conf t  ipv6 unicast-routing  ip route 192.168.2.0 255.255.255.0 s0/1/0  ip route 0.0.0.0 0.0.0.0 s0/1/1  ip route 33.0.0.0 255.0.0.0 g0/0/0  ipv6 route 2001:CAFE::/64 s0/1/0  ipv6 route ::/0 s0/1/1  ip nat inside source static 20.0.0.2 33.222.44.80  int s0/1/0  ipv6 enable  ip add 10.0.0.2 255.0.0.0  ipv6 add 2001:A::2/64  ip nat outside  no sh  int s0/1/1  ipv6 enable  ip add 66.222.44.77 255.0.0.0  ipv6 add 2001:BABA::1/64  ip nat outside  no sh  int g0/0/0  ipv6 enable  ip add 20.0.0.1 255.0.0.0  ipv6 add 2001:B::1/64  ipv6 add FE80::1 link-local  ip nat inside  no sh  ip access-list extended PINGIN  deny icmp any any echo  permit ip any any  ex  ipv6 access-list PINGINv6  deny icmp any any  permit ipv6 any any  int s0/1/1  ip access-group PINGIN in  ipv6 traffic-filter PINGINv6 in |  |
| … |  |  |

**HTTP szerver konfiguráció lényegi részei:**

|  |  |  |
| --- | --- | --- |
| PasswordAuthentication no  PermitRootLogin no  AddressFamily inet  Port 2222 | | /etc/ssh/sshd\_config |
| chain input {  # accept any localhost traffic  # accept traffic originated from us  # drop invalid packets  ct state invalid counter log prefix "riasztas" drop  # accept ssh, http, and https  # accept icmp  # count and reject everything else  chain forward {  type filter hook forward priority 0; policy drop;  }  chain output {  type filter hook output priority 0; policy accept;  } | | nftables |
| <VirtualHost \*:80>  sudo chown -R www-data:www-data /var/www/html/dwsbt.site/public\_html  sudo chmod -R 755 /var/www/html/dwsbt.site/public\_html  sudo a2ensite dwsbt.site  sudo a2dissite 000-default.conf | | apache2 - http |
|  | | |
| **név (nevek):** | X | |
| **osztály/csoport:** | X | |
| **munkaállomások nevei:** |  | |
| **elérhetőség:** | X | |
| **dátum:** | X | |

**Tartalomjegyzék**

…

…