Baranya Vármegyei SZC Mohácsi Radnóti Miklós Technikum és Szakképző Iskola

VIZSGAREMEK

Készítettek:

Szalai Márk Csaba

Klaics János

Jordán Kristóf

Mohács

2025

Baranya Vármegyei SZC Mohácsi Radnóti Miklós Technikum és Szakképző Iskola

Szakma megnevezése:

A szakma azonosító száma:

Vizsgaremek

CureNet

Készítettek:

Szalai Márk Csaba

Klaics János

Jordán Kristóf

Mohács

Feladat rövid ismertetése

Bevezetés

A CureNetFc projekt célja, hogy egy olyan digitális hálózati rendszert hozzon létre, amely biztonságos megoldást kínál a labdarúgó játékosok felfedezésére, adatelemzésére és csapatokhoz történő eljuttatására. A rendszer létrehozásával célunk a sportvilág digitalizálása, valamint a futballpiac szereplői számára egy hatékonyabb, átláthatóbb, és biztonságosabb környezet biztosítása. Az alkalmazás különösen nagy figyelmet fordít a jogosultságok kezelésére, valamint a hálózati biztonságra, hogy az illetéktelen hozzáférést megakadályozza.

Cél

A CureNetFc projekt egyik fő célja egy olyan biztonságos hálózati rendszer kialakítása, amely lehetőséget biztosít a futballcsapatok és a játékosok számára, hogy közvetlenül és megbízhatóan kapcsolatba léphessenek egymással. A rendszer funkcionalitása lehetővé teszi a játékosok teljesítményének nyomon követését, a csapatok által történő keresést és szűrést, valamint a kommunikációs csatornák biztonságos fenntartását. Az alkalmazás fejlesztésénél kiemelt szempont volt a könnyű kezelhetőség , a felhasználóbarát felület, valamint a rendszer skálázhatósága, amely lehetőséget biztosít a jövőbeli fejlesztésekhez.

Jövőbeli tervek

A projekt jövőbeli fejlesztési irányai között szerepel a rendszer további funkcionális bővítése, amely lehetőséget biztosít a felhasználók szélesebb körű kiszolgálására. A tervek között szerepel egy weboldal bevezetése, amely segítségével a játékosok és csapatok gyorsan és egyszerűen elérhetik az információkat, valamint interaktívan használhatják a szolgáltatásokat.

A jövőben tervezett bővítések során figyelembe vesszük a felhasználói visszajelzéseket, valamint a technológiai fejlődéseket, hogy a lehető legjobb élményt biztosítsuk a sportvilág szereplői számára. Hosszútávú célunk a rendszer további skálázhatósága és nemzetközi piacra történő kiterjesztése, amely lehetővé tenné, hogy a CureNetFc egy globális megoldásként segítse a futballpiac szereplőit.

Alkalmazott technológiák

Topológia: A hálózat hibrid topológiát használ, amely a központi routerekhez csatlakozó switcheken keresztül biztosítja a végfelhasználói eszközök kapcsolatát. Ez a topológia jól skálázható, könnyen kezelhető és lehetővé teszi a forgalom hatékony irányítását. A topológia kialakításakor figyelembe vettük a vállalat méretét, a felhasználók számát és az adatforgalom mennyiségét. A hibrid topológia előnyei közé tartozik a redundancia, a hibaelkülönítés és a könnyű bővíthetőség. A topológia kialakításakor figyelembe vettük a hálózat biztonsági követelményeit is.

Használt eszközök kiválasztása

A hálózat kiépítéséhez és üzemeltetéséhez a következő Cisco eszközöket és szoftvereket használtuk:

Routerek:
A Cisco 1841 router nagy teljesítményt és biztonságot nyújt a hálózati forgalom irányításához. Moduláris felépítésének köszönhetően könnyen bővíthető az igényeknek megfelelően. A router támogatja a különböző routing protokollokat, biztonsági funkciókat és a QoS (Quality of Service) beállításokat, lehetővé téve a hatékony és megbízható hálózati működést.

Switchek:
A Cisco Catalyst 2960 sorozatú switch intelligens Layer 2 switching képességeket biztosít a hálózati kapcsolatokhoz, valamint korlátozott Layer 3 funkciókat. A Catalyst 2960 IOS15 modell nagy portszámmal rendelkezik, és támogatja a VLAN-okat, a QoS-t és a különböző biztonsági funkciókat, például az ACL-eket és a port security-t. A switchek menedzselhetők Cisco Prime Infrastructure vagy más hálózati menedzsment eszközökkel, biztosítva a hatékony felügyeletet és konfigurációkezelést.

Tűzfalak:
Cisco ASA (Adaptive Security Appliance) sorozat, amely átfogó biztonsági védelmet nyújt a hálózatnak a külső támadásokkal szemben. Az ASA tűzfalak hardveres és szoftveres védelemmel rendelkeznek, és támogatják a tűzfal funkciókat, a behatolásérzékelést és -megelőzést (IDS/IPS), a VPN-t és az alkalmazásszintű szűrést.

VPN eszközök:
Cisco VPN kliensek és szerverek, amelyek biztonságos távoli hozzáférést biztosítanak a hálózathoz. A Cisco VPN kliensek és szerverek támogatják a különböző VPN protokollokat, mint például az

IPsec, az SSL és az L2TP. A VPN kapcsolatok titkosítást és hitelesítést biztosítanak, így védve az adatokat a jogosulatlan hozzáféréstől.

Hálózati operációs rendszer:

Cisco IOS (Internetwork Operating System), amely a Cisco eszközökön futó, fejlett hálózati funkciókat biztosító operációs rendszer. A Cisco IOS egy

parancssoros interfészt (CLI) és egy grafikus felhasználói felületet (GUI) is kínál a hálózat konfigurálásához és menedzseléséhez.

Hálózati menedzsment szoftver:

Cisco Prime Infrastructure, amely átfogó hálózatfelügyeleti és -kezelési képességeket biztosít. A Cisco Prime Infrastructure segítségével monitorozhatjuk a hálózat állapotát, konfigurálhatjuk az eszközöket, hibaelhárítást végezhetünk és jelentéseket készíthetünk.

Egyéb technológiák

1. **Git**

- A Git egy elosztott verziókezelő rendszer, amely segíti a fejlesztőket a kódbázis nyomon követésében, változtatások kezelésében és együttműködésben a csapaton belül. Az elosztott jellege lehetővé teszi a párhuzamos fejlesztést, valamint a könnyű visszatérési pontok (commit) készítését és visszaállítását

2. **Jira**

- A Jira egy olyan project management eszköz, amely lehetővé teszi a csapatoknak a projektjeik nyomon követését, feladatok kezelését és a fejlesztési folyamatok hatékony szervezését. Az eszköz segíti a feladatok rendszerezését, a prioritások meghatározását és a csapat tagjainak közötti kommunikációt.

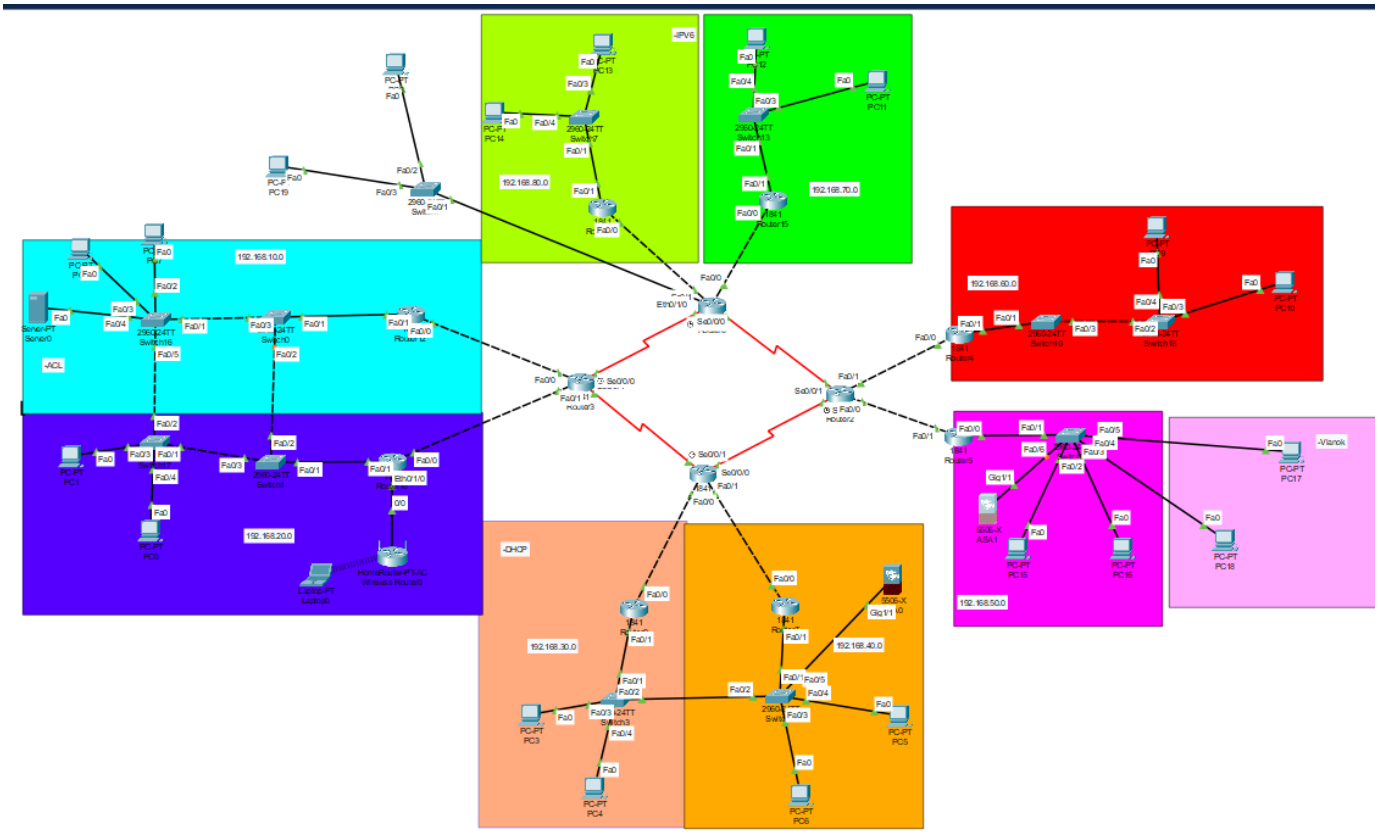
Hálózat Rövid Magyarázata

A hálózat megfelelő működéséhez elengedhetetlen, hogy az egyes eszközök hatékonyan és biztonságosan kommunikáljanak egymással. Ennek érdekében a hálózat felépítése úgy lett kialakítva, hogy biztosítsa a gyors adatáramlást és a jogosulatlan hozzáférések elleni védelmet.

A rendszer alapját különálló hálózati szegmensek alkotják, amelyek biztosítják a szerverek, kliensgépek és adminisztratív eszközök közötti hatékony kommunikációt. A VLAN-ok és ACL-ek alkalmazásával a forgalom megfelelően szabályozott, így az adatok csak az arra jogosult eszközök között áramlanak.

A hálózat megfelelő útválasztási mechanizmusokat és biztonsági intézkedéseket alkalmaz, hogy garantálja a stabil és megbízható kapcsolatot. A szerverek a webalkalmazás és az adatbázis kiszolgálásáért felelősek, amelyeket tűzfalak és hozzáférés-kezelési megoldások védenek.

Az alkalmazott technológiák és hálózati megoldások biztosítják, hogy a rendszer könnyen skálázható, megbízható és biztonságos legyen, lehetővé téve a felhasználók számára a szolgáltatások zökkenőmentes elérését.



A hálózat több fő részre osztható, mindegyik különböző funkcionális területeket képvisel:

Hálózat ismertetése

A Épület Hálózati Ismertetése

Az A épület a CureNetFc projekt egyik kulcsfontosságú hálózati helyszíne, ahol a rendszert közvetlenül tesztelik és használják a futballcsapatok, valamint az adatelemző csapatok. Az épület hálózata egy hibrid topológiára épül, amely központi routereken és switcheken keresztül biztosítja a kapcsolatokat a végfelhasználói eszközök számára.
A hálózat kialakításánál kiemelt szerepet kapott a biztonság. Az ACL (Access Control List) beállítására különös figyelmet fordítottunk annak érdekében, hogy szabályozzuk a forgalomáramlást, és megakadályozzuk az illetéktelen hozzáférést.

Az ACL szerepe az A épületben

Az A épület hálózatában az ACL-ek kulcsfontosságúak, mert biztosítják, hogy a szerveren tárolt szenzitív adatokat csak az arra jogosult felhasználók érhetik el. A szegmentált VLAN-ok közötti kommunikáció korlátozására is használatra kerülnek, hogy a különböző részlegek csak a számukra releváns adatforgalmat láthassák.

B Épület Hálózati Ismertetése

A B épület a CureNetFc projekt egyik kritikus része, mivel itt található a DHCP szerver, amely dinamikusan kiosztja az IP-címeket a hálózati eszközök számára. A hálózat kialakítása lehetővé teszi, hogy a csatlakozó kliensek automatikusan IP-címet kapjanak, így nem szükséges manuálisan konfigurálni minden egyes eszközt. Ez különösen fontos egy olyan rendszerben, ahol folyamatosan változhatnak a csatlakozó eszközök és felhasználók.

A DHCP szerepe a B épületben

A DHCP (Dynamic Host Configuration Protocol) lehetővé teszi az automatikus IP-cím kiosztást, amely megkönnyíti a hálózat kezelését. Biztosítja, hogy minden eszköz egyedi IP-címet kapjon, elkerülve az IP-ütközéseket. B épület kliensei így gyorsan és hatékonyan csatlakozhatnak a hálózathoz.

C Épület Hálózati Ismertetése

A C épület a CureNetFc projekt egyik meghatározó hálózati helyszíne, ahol különböző VLAN-ok biztosítják az elkülönített hálózati kommunikációt és az adatbiztonságot. A hálózatot **rétegzett architektúra** jellemzi, amelyben switch-ek és routerek kezelik a forgalmat. Az egyes VLAN-ok külön alhálózatokat használnak, amelyeket a központi eszközök irányítanak. Az infrastruktúra kiemelten kezeli a forgalomszabályozást, az eszközök elérhetőségét és az illetéktelen hozzáférések megakadályozását.

VLAN szerepe a C épületben

A VLAN-ok segítségével a hálózat hatékonyabb és biztonságosabb lett, mivel lehetővé teszik a forgalom szegmentálását és az egyes részlegek izolálását. A különböző VLAN-ok korlátozzák az illetéktelen hozzáférést és növelik a hálózat teljesítményét azzal, hogy csökkentik a felesleges adatforgalmat. A biztonsági VLAN védi az érzékeny adatokat, míg a vendéghálózat biztosítja a külső eszközök elkülönített kapcsolódását. Az adminisztrációs VLAN a hálózatfelügyeletet és karbantartást szolgálja, garantálva a stabil működést.

D Épület Hálózati Ismertetése

A D épület a CureNetFc projekt egyik kiemelt helyszíne, ahol az IPv6-alapú hálózat biztosítja a modern és jövőbiztos kommunikációt. A hálózat kialakítása moduláris topológiát követ, amely switch-ek és routerek segítségével optimalizálja az adatáramlást. A szegmentáció és a címzési struktúra az IPv6 előnyeit kihasználva lehetővé teszi a hatékonyabb címkezelést és nagyobb skálázhatóságot. A forgalomirányítás dinamikusan történik, biztosítva az alacsony késleltetést és a stabil működést.

IPv6 szerepe a D épületben

Az IPv6 bevezetésével a D épület hálózata jövőálló és biztonságosabb lett, mivel az új címzési rendszer nagyobb kapacitást és hatékonyabb forgalomkezelést tesz lehetővé. Az automatikus címkonfiguráció leegyszerűsíti az eszközök hálózati beállítását, miközben a fejlettebb titkosítási mechanizmusok növelik az adatvédelem szintjét. Az IPv6 multicast és QoS támogatása elősegíti a jobb sávszélesség-kezelést és a valós idejű kommunikáció hatékonyságát.

Fejlesztés módszertan

Scrum

1. Rendszeres fejlesztési ciklusok:

- A Scrum keretrendszer rendszeres, általában két-három hetes időszakokra tervezett fejlesztési ciklusokat biztosított számunkra. Ez lehetővé tette, hogy gyorsan és rendszeresen hozzáférjünk a fejlesztett funkcionalitásokhoz, és azonnali visszajelzést kapjunk a csapat és az érintettek részéről.

2. Csapatmunka és transzparencia:

- A Scrum keretrendszer elősegítette a hatékony csapatmunkát és átláthatóságot a projektben. A rendszeres Scrum értekezletek és a projekt backlog frissítése révén minden csapattag számára világos volt a projekten belüli állapot és prioritások.

3. Rugalmasság a Változásokra:

- A Scrum módszertan lehetővé tette számunkra, hogy rugalmasan alkalmazkodjunk a változásokhoz a projekt folyamán. Az iteratív fejlesztési ciklusok és a rendszeres retrospektív értekezletek révén könnyen integráltuk a visszajelzéseket, és gyorsan reagálhattunk az esetleges változásokra, optimalizálva ezzel a projekt irányát és funkcionalitásait.

Elvégzett hálózati tesztelések

A hálózat megfelelő működésének biztosítása érdekében többféle tesztelési módszert alkalmaztunk, amelyek a rendszer stabilitását, teljesítményét és biztonságát vizsgálták. A tesztelés során az alapvető funkcionális ellenőrzésektől kezdve a teljesítménytesztekenen át a hibatűrési próbákig különböző eljárásokat hajtottunk végre.

Manuális hálózati tesztelés:

- A manuális tesztelés során a hálózati infrastruktúra egyes elemeit – például routereket, switcheket és végpontokat – kézi konfigurációval és monitorozással ellenőriztük.
- Teszteltük az alapvető hálózati kapcsolatokat, az eszközök közötti kommunikációt, valamint a csomagok megfelelő továbbítását.
- A manuális ellenőrzések célja az volt, hogy megbizonyosodjunk az eszközök helyes konfigurációjáról és a hálózat működőképességéről.

Automatizált hálózati tesztelés:

- Az automatizált tesztelés során szkripteket és hálózati diagnosztikai eszközöket (pl. ping, traceroute, packet capture) használtunk az adatok gyors és pontos elemzésére.
- A hálózati forgalmat különböző terhelési szinteken vizsgáltuk, hogy ellenőrizzük a sávszélesség-kezelést és a késleltetési értékeket.
- A tesztelés során figyelemmel kísértük az útvonalválasztási protokollok működését, a csomagvesztést és az átviteli időket is.

A tesztelések jelentősége

Manuális tesztelés jelentősége:

- A manuális ellenőrzések biztosították, hogy a hálózat konfigurációja helyesen valósuljon meg, és minden eszköz megfelelően működjön.
- Segített feltárni az esetleges hibákat, például a helytelen kábelezést, konfigurációs eltéréseket vagy eszközhibákat.

Automatizált tesztelés jelentősége:

- Az automatizált tesztelés lehetővé tette a gyors és pontos hibakeresést, valamint a teljesítményproblémák észlelését.
- A hálózat skálázhatóságának és terhelhetőségének ellenőrzésére szolgált, biztosítva ezzel a megfelelő sávszélességet és válaszidőt.

Topológia és hálózati eszközök kiválasztása

Topológia:

A hálózat egy hibrid topológiára épül, amelyben a végfelhasználói eszközök kapcsolódását központi routerekhez csatlakoztatott switchek biztosítják. Ez a struktúra hatékony forgalomirányítást,

egyszerű kezelhetőséget és jó skálázhatóságot tesz lehetővé. A topológia tervezésekor figyelembe vettük a cég méretét, a felhasználók számát, valamint a hálózati forgalom nagyságát. A hierarchikus felépítés előnyei közé sorolható a hibatűrés, a gyors hibaelhárítás, valamint a könnyű bővíthetőség. Emellett a kialakítás során a biztonsági szempontokat is figyelembe vettük.

Hálózati eszközök:

Az eszközök kiválasztásakor olyan szempontokat vettünk figyelembe, mint a teljesítmény, biztonság, költséghatékonyság és skálázhatóság. A Cisco eszközök megfeleltek ezeknek az elvárásoknak, ráadásul széles körben elterjedtek a vállalati hálózatokban. Az eszközök specifikációit a cég igényeihez igazítottuk, beleértve a szükséges portszámokat, a támogatott hálózati protokollokat és a beépített biztonsági funkciókat. Emellett ügyeltünk arra is, hogy a választott eszközök hosszú távon támogassák a hálózat bővítését és fejlesztését.

IP-címzés és alhálózatok kialakítása

IP-címzés:

A hálózatban az RFC 1918 szabványnak megfelelő privát IP-címeket alkalmaztuk. Az IP-címek kiosztásakor figyelembe vettük a hálózat struktúráját és a különböző részlegek egyedi igényeit. Minden részleg számára külön alhálózatot hoztunk létre, amelyhez egyedi IP-tartományt rendeltünk. Az IP-címek dinamikus kiosztását egy DHCP szerver végzi, amely automatikusan osztja ki az IP-címeket a csatlakoztatott eszközök számára. A DHCP konfiguráció során beállítottuk a kiosztandó IP-címtartományokat, az IP-bérleti időt, valamint megadtuk az alapértelmezett átjáró és a DNS szerverek címét. Az állandó IP-címeket olyan eszközök számára tartottuk fenn, amelyek folyamatos elérhetőséget igényelnek, például a szerverek és a hálózati nyomtatók.

Alhálózatok:

A hálózat hatékonyabb kezelése, a biztonság növelése és a teljesítmény optimalizálása érdekében a hálózatot kisebb alhálózatokra osztottuk. Minden alhálózat egy különálló IP-címtartományt használ, és a forgalom irányítása az alhálózatok között routereken keresztül történik. Az alhálózatok kialakítása során figyelembe vettük az egyes részlegek működési igényeit, valamint a hálózat logikai felépítését. A biztonságos kommunikáció érdekében az alhálózatok közötti adatforgalmat tűzfalakkal és hozzáférési listákkal (ACL) szabályoztuk. Az alhálózatok megtervezésekor szem előtt tartottuk a hálózat jövőbeli bővítésének lehetőségét, hogy rugalmasan alkalmazkodhassunk a változó igényekhez.

VLAN-ok és szegmentálás

Szegmentálás

A hálózat szegmentálásának bevezetése jelentős mértékben növelte mind a biztonságot, mind a teljesítményt. A VLAN-ok és az alhálózatok kialakítása egyaránt a szegmentáció részét képezte, lehetővé téve a különböző részlegek forgalmának elkülönítését. Ez segített megakadályozni a jogosulatlan hozzáférést és a hálózati problémák szélesebb körű terjedését. A forgalom elkülönítésével csökkent a hálózat terhelése, mivel az adatáramlás kizárólag a releváns alhálózatokra korlátozódott. A szegmentáció kialakításánál figyelembe vettük a vállalat biztonsági szabályait és a vonatkozó jogszabályokat, biztosítva ezzel a megfelelő védelmet mind belső, mind külső fenyegetésekkel szemben.

Routing Megoldások

IP Routing

A hálózat forgalmának irányítása érdekében IP alapú útvonalválasztást (IP Routing) alkalmaztunk. Az útvonalválasztás célja, hogy az adatcsomagokat a leghatékonyabb és legbiztonságosabb úton juttassa el a célállomásra. A konfiguráció során statikus és dinamikus útvonalakat egyaránt beállítottunk, hogy biztosítsuk a hálózat stabil és gyors működését.

A statikus útvonalakat olyan kritikus kapcsolatokhoz használtuk, ahol az útvonalak előre meghatározottak, és nem változnak gyakran. Ezeket a routerek manuálisan konfigurálják, így az útvonalak kiszámíthatóak és könnyen ellenőrizhetőek. A dinamikus útvonalválasztás mellett RIP (Routing Information Protocol) és EIGRP (Enhanced Interior Gateway Routing Protocol) protokollokat is alkalmaztunk, amelyek automatikusan frissítik az útvonalakat a hálózat állapotának változásai alapján.

A hálózat megbízhatóságának növelése érdekében redundáns útvonalakat állítottunk be, amelyek hiba esetén alternatív utat biztosítanak az adatok számára. A routerek konfigurációja magában foglalta az interfészek beállítását, a prioritások meghatározását és a szükséges útvonalak

megadását. Az IP Routing alkalmazása lehetővé tette a hálózat stabil és hatékony működését, amely dinamikusan alkalmazkodik a terheléshez és a hálózati körülményekhez.

Hálózatbiztonság és Hozzáférés-vezérlés

ACL-ek és forgalomszűrés

A hálózati biztonság fenntartása érdekében hozzáférés-vezérlési listákat (ACL – Access Control Lists) alkalmaztunk a forgalom szabályozására. Az ACL-ek segítségével pontosan meghatároztuk, hogy milyen forrásból és milyen célba irányuló forgalmat engedélyezünk vagy tiltunk. Az ACL-eket routereken és switcheken konfiguráltuk, hogy védelmet nyújtsanak a jogosulatlan hozzáférések és a potenciálisan káros hálózati forgalom ellen. Az ACL konfiguráció tartalmazta a szabályok létrehozását, az interfészekhez való hozzárendelést, valamint a bejövő és kimenő forgalom kezelését. Az ACL-ekkel történő forgalomszűrés jelentős védelmet biztosított a DoS (Denial of Service) támadásokkal és egyéb fenyegetésekkel szemben.

VPN beállítás (Távoli elérés és Site-to-Site kapcsolatok)

A biztonságos távoli hozzáférés és telephelyek közötti kommunikáció érdekében VPN (Virtual Private Network) technológiát vezettünk be. Két különböző VPN megoldást alkalmaztunk:

- **Távoli elérés VPN**: A távoli dolgozók számára biztonságos kapcsolatot biztosítottunk a vállalati hálózathoz. A VPN klienst futtató eszközök titkosított csatornán keresztül kapcsolódtak a vállalati infrastruktúrához, megakadályozva az érzékeny adatok kiszivárgását. A konfiguráció során beállítottuk a hitelesítési módszereket és a titkosítási protokollokat, amelyek biztosították az adatok biztonságát.
- **Site-to-Site VPN**: A vállalat különböző telephelyeit biztonságos VPN alagutakon keresztül kapcsoltuk össze, biztosítva az adatok titkosított továbbítását. A Site-to-Site VPN Cisco ASA tűzfalakon keresztül valósult meg, amelyek VPN gateway-ként működnek, garantálva az adatbiztonságot és a hálózati integritást.

Cisco tűzfalak alkalmazása

A hálózat védelmének egyik központi elemeként Cisco ASA tűzfalakat implementáltunk. A tűzfalak valós időben ellenőrzik a hálózati forgalmat, blokkolják a nem kívánt kapcsolatokat és megelőzik a jogosulatlan hozzáférést. A tűzfal konfiguráció során meghatároztuk a biztonsági szabályokat, a forgalomszűrési beállításokat és a behatolásérzékelési mechanizmusokat. A Cisco ASA tűzfalak

fejlett funkciókat biztosítanak, beleértve az alkalmazásszintű szűrést, vírusvédelmet és behatolásmegelőzést (IPS). A tűzfalak naplózási és monitoring funkciói

lehetővé tették a hálózat biztonsági állapotának folyamatos felügyeletét, elősegítve a proaktív védelmet a külső és belső fenyegetések ellen.

Hálózatfelügyelet és Hibakeresés

Diagnosztikai eszközök és módszerek

A hálózat hatékony felügyelete és a hibák gyors elhárítása érdekében különböző diagnosztikai eszközöket használunk, amelyek segítenek az elérhetőségi és kapcsolati problémák azonosításában. A leggyakrabban alkalmazott eszközök és parancsok az alábbiak:

- **Ping**: Az ICMP (Internet Control Message Protocol) segítségével ellenőrzi, hogy egy adott eszköz elérhető-e a hálózaton. A válaszidő mérése segíthet a késleltetés vagy csomagvesztés diagnosztizálásában. A ping egyszerű, de hatékony eszköz a hálózati kapcsolatok alapvető tesztelésére.
- **Traceroute**: Lehetővé teszi a hálózati csomagok által bejárt útvonal feltérképezését a forrástól a célállomásig. Ez az eszköz segít azonosítani a hálózatban található akadályokat vagy torlódási pontokat, amelyek hatással lehetnek az adatátvitelre. Windows környezetben a `tracert`, Linux és macOS rendszereken a `traceroute` parancs használható.
- **Ipconfig (Windows) / Ifconfig (Linux, macOS)**: Ezek a parancsok részletes információt adnak a helyi hálózati adapter beállításairól, beleértve az IP-címet, az alhálózati maszkot és az alapértelmezett átjárót. Hasznosak az IP-címzés és a kapcsolatellenőrzés során.
- **Netstat**: Megmutatja az aktuálisan nyitott hálózati kapcsolatokat, portokat és a hálózati interfészek állapotát. Ezzel az eszközzel azonosíthatók a nem kívánt hálózati kapcsolatok és a hálózat leterheltsége.
- **Nslookup / Dig**: Ezek az eszközök a DNS-problémák diagnosztizálására szolgálnak. Az `nslookup` segítségével ellenőrizhető egy domain név IP-címre történő feloldása, míg a `dig` (Linux/Mac) részletesebb DNS-információkat biztosít.
- **Wireshark**: Egy fejlett hálózati forgalomelemző eszköz, amely lehetővé teszi a hálózaton áthaladó csomagok valós idejű vizsgálatát. Segítségével részletes elemzést végezhetünk a hálózati protokollok és kommunikációs folyamatok kapcsán.

Ezek az eszközök együttesen biztosítják a hálózat állapotának felügyeletét és a gyors hibakeresést, minimalizálva a leállások időtartamát és javítva a rendszer stabilitását.

Implementáció és Tesztelés

Részletes tesztelési terv és végrehajtás

A tesztelési terv célja, hogy biztosítsa a rendszer megfelelő működését, és feltárja az esetleges hibákat még az éles üzembe helyezés előtt. A tesztelés során ellenőrizni kell a hálózat alapvető működését, az alkalmazások elérhetőségét, a biztonsági mechanizmusok hatékonyságát, valamint a teljesítményt és a terhelhetőséget. A megfelelő tesztelési folyamat elengedhetetlen a stabil és megbízható működéshez.

A tesztelési módszerek közé tartozik a funkcionális tesztelés, amely során vizsgáljuk, hogy a rendszer megfelelően működik-e, és a hálózati eszközök képesek-e kommunikálni egymással. A teljesítménytesztek célja, hogy meghatározzák a hálózat sebességét és terhelhetőségét különböző körülmények között. A biztonsági tesztelés során a rendszer védelmét ellenőrizzük a külső és belső fenyegetésekkel szemben, míg a terhelési tesztek segítségével szimuláljuk a nagyobb terhelés alatti működést, hogy felmérjük a stabilitást és a skálázhatóságot.

A tesztelési környezet összeállítása kulcsfontosságú, hiszen a tesztelési eredmények csak akkor lesznek relevánsak, ha a környezet hasonlít az éles üzemhez. Ehhez szükség lehet különböző hardver- és szoftvereszközökre, például tesztszerverekre, klienseszközökre, hálózati analizátorokra és monitorozó rendszerekre.

A tesztelési ütemtervnek részletesen tartalmaznia kell a tesztelési szakaszokat, a végrehajtás időpontjait és a felelős személyeket. Fontos, hogy a tesztek megfelelő sorrendben történjenek, így biztosítva a folyamatos ellenőrzést és visszacsatolást.

A tesztelési forgatókönyvek kidolgozása elengedhetetlen ahhoz, hogy a tesztek következetesen és pontosan végrehajthatók legyenek. Ezeknek tartalmazniuk kell a konkrét vizsgálati lépéseket, az elvárt eredményeket és a tesztelési környezet leírását. Ide tartozhat például a kapcsolati teszt, amely ellenőrzi a hálózati kapcsolatokat, az adatátviteli teszt, amely méri a sebességet és stabilitást, valamint az alkalmazások megfelelő működésének ellenőrzése és a biztonsági protokollok tesztelése.

Az elvárt eredmények egyértelmű meghatározása szükséges annak érdekében, hogy a tesztelés során egyértelmű következtetéseket lehessen levonni. Ilyen elvárások lehetnek például a sikeres csatlakozás a hálózathoz, az adatátviteli sebesség megfelelősége vagy a biztonsági intézkedések hatékonysága.

A tesztelési dokumentáció szintén fontos része a folyamatnak, hiszen ennek segítségével rögzíteni lehet a tesztelés során szerzett tapasztalatokat, az esetleges hibákat és az azokhoz kapcsolódó javítási javaslatokat. A dokumentációnak tartalmaznia kell a tesztjegyzőkönyveket, a hibajelentéseket és az összegzéseket, amelyek alapján a rendszer végső értékelése elvégezhető.

A tesztelési folyamat végrehajtása során elengedhetetlen a terv pontos követése és a kapott eredmények szisztematikus dokumentálása. Az eredmények kiértékelése után szükség esetén javításokat kell végrehajtani, majd a rendszer ismételt tesztelése következik. Amennyiben minden kritérium teljesül, a rendszer készen áll az éles üzembe helyezésre.

Dokumentáció és Karbantartás

·Konfigurációs mentések és verziókezelés :

A konfigurációs mentéseket automatizálhatjuk TFTP (Trivial File Transfer Protocol) vagy SFTP (Secure File Transfer Protocol) szerver segítségével. A verziókezeléshez használhatunk olyan eszközöket, mint a Git vagy a Mercurial. A konfigurációs mentések és a verziókezelés lehetővé teszik a hálózat gyors helyreállítását hiba esetén és a konfigurációs változások nyomon követését.

Hibajelentések és naplózás:

A naplózási beállítások konfigurálása magában foglalja a naplózási szint beállítását, a naplózási cél megadását és a naplózási üzenetek formátumának beállítását. A központi naplózási szerverre küldött naplókat elemezhetjük olyan eszközökkel, mint a Syslog vagy az ELK stack (Elasticsearch, Logstash, Kibana). A naplózás lehetővé teszi a hálózat biztonsági eseményeinek nyomon követését, a hibák azonosítását és a hálózat működésének elemzését. A naplók rendszeres áttekintése és elemzése segít a hálózati problémák proaktív azonosításában és a biztonsági incidensek megelőzésében.

·Jövőbeli fejlesztési tervek:

A jövőbeli fejlesztések tervezésekor figyelembe kell venni a hálózat jelenlegi állapotát, a várható növekedést és az új technológiák lehetőségeit. A fejlesztési javaslatok lehetnek például a hálózat sebességének növelése, a biztonság megerősítése, a felhő alapú szolgáltatások bevezetése vagy a mobil eszközök támogatásának javítása. A fejlesztési javaslatoknak tartalmazniuk kell a megvalósítási terveket, az erőforrásigényt és a költségbecslést. A jövőbeli fejlesztések megvalósítása előtt fontos a részletes tervezés és a tesztelés. A fejlesztési javaslatoknak összhangban kell lenniük a vállalat stratégiai céljaival és az üzleti igényekkel. A fejlesztési javaslatok megvalósítása hozzájárulhat a hálózat hatékonyságának, biztonságának és versenyképességének javításához.

Csapatmunka:

Szerepek

Jordán Kristóf vállalt szerepei és felelősségi területei a következők voltak a projekt során:

1. **Project manager (Projektmenedzser) :**
   - Feladata a projekt egészének irányítása és felügyelete.
   - Koordinálta a csapatmunkát és ütemezte a fejlesztési folyamatokat.
   - Hatékony kommunikáció biztosítása a csapattagok között és a projekt érintettjeivel.

2. **Hálózati infrastruktúra-fejlesztő:**
   - A hálózati architektúra megtervezése és implementálása.
   - A hálózati eszközök (routerek, switchek, szerverek) konfigurálása és tesztelése.
   - A hálózati kapcsolatokat biztosító protokollok beállítása és optimalizálása.

3. **Biztonsági tesztelő:**
   - A hálózat sebezhetőségeinek feltérképezése és biztonsági rések felderítése.
   - A behatolásvédelem és tűzfalak tesztelése különböző támadási szcenáriók alapján.
   - Az eredmények dokumentálása és javítási javaslatok kidolgozása.

Szalai Márk Csaba vállalt szerepei és felelősségi területei a következők voltak a projekt során:

1. **Rendszeradminisztrátor**
   - A szerverek és hálózati eszközök karbantartása és optimalizálása.
   - A hálózati hozzáférések kezelése és jogosultságok beállítása.
   - A rendszeres frissítések és javítások telepítése a stabilitás fenntartása érdekében.

2. **Hálózati teljesítmény-elemző:**
   - A hálózati sávszélesség és forgalom monitorozása.
   - A teljesítményproblémák azonosítása és megoldási javaslatok kidolgozása.
   - A hálózati forgalmi minták elemzése és a terheléselosztás optimalizálása.

3. **Automatizált tesztelő**

- A hálózati eszközök és szolgáltatások automatikus teszteléséhez szükséges szkriptek fejlesztése.
- Tesztelési környezet kialakítása és a folyamatok automatizálása.
- Hibák dokumentálása és jelentések készítése a fejlesztési csapat számára.

Klaics János vállalt szerepei és felelősségi területei a következők voltak a projekt során:

1. **Hálózati mérnök:**
   - A hálózati topológia tervezése és kivitelezése.
   - Az IP-címzés és alhálózatok konfigurálása az optimális működés érdekében.
   - A redundancia és a hibatűrő mechanizmusok beépítése a hálózati infrastruktúrába.

2. **Hálózati adatbázis-adminisztrátor:**
   - A hálózati konfigurációkat és naplófájlokat tároló adatbázisok kezelése.
   - A hálózati események és forgalmi adatok elemzése és archiválása.
   - Biztonsági mentések és helyreállítási folyamatok kidolgozása.

3. **Hálózati hibakereső és diagnosztikai szakértő:**
   - A hálózati hibák gyors beazonosítása és elhárítása.
   - A csomagforgalom analizálása és a hálózati eszközök hibás működésének detektálása.
   - A problémák dokumentálása és a javasolt megoldások tesztelése.

A projekt során szerzett tapasztalatok alapján megállapítottuk, hogy az agilis projektmenedzsment alkalmazása kiemelkedően hatékony volt rugalmas és hatékony fejlesztési folyamatok kialakításában. Az agilis megközelítés hasznosnak bizonyult a változó követelmények kezelésében, és a csapatmunka során szerzett tapasztalatok alapján azonosítottunk területeket, amelyeken a jövőben fejleszteni szeretnénk, például a projektmenedzsment finomhangolását

Jövőbeli terveink

Hálózati adminisztrációs rendszer:

A fejlesztési tervek között szerepel egy átfogó hálózatfelügyeleti rendszer kialakítása, amely lehetővé teszi a hálózat teljes körű monitorozását és az eszközök kezelését. Ez a rendszer biztosítja majd a valós idejű forgalomelemzést, a hozzáférési jogosultságok adminisztrációját, valamint az egyes hálózati eszközök állapotának ellenőrzését. A cél az, hogy egy könnyen kezelhető, biztonságos adminisztrációs felület jöjjön létre, amely támogatja a gyors hibaelhárítást és az optimális működést.

Biztonságos kommunikációs rendszer:

A projekt egyik kiemelt fejlesztési iránya egy új, biztonságos üzenetküldési protokoll bevezetése a hálózaton belüli kommunikáció optimalizálására. Az új rendszer lehetővé teszi a titkosított adatátvitelt, amely biztosítja az érzékeny információk védelmét a hálózaton belül és kívül. A megoldás támogatni fogja a valós idejű csoportos és egyéni kommunikációt, valamint az adatok naplózását a jobb átláthatóság érdekében. A cél egy gyors, megbízható és könnyen integrálható üzenetkezelő infrastruktúra kialakítása.

Ez a fejlesztés nemcsak növeli a hálózat biztonságát és stabilitását, hanem hatékonyabb adatkezelést is lehetővé tesz, ezzel javítva az általános hálózati teljesítményt és a felhasználói élményt.