Üdvözlünk mindenkit mi vagyunk az Innotech Networks kft. A cégünk hálózat tervezésével, kivitelezésével és rendszerüzemeltetéssel foglalkozik különböző iparágakon belül, mint például egészségügy, oktatás, kereskedelem.

Az Innotech Networks Magyarország egyik legmegbízhatóbb legsokoldalúbb szolgáltatását nyújtja hálózati téren több mint 100 elégedett ügyféllel karöltve. Cégünk folyamatosan fejlődik így mindig a legújabb legfejlettebb technológiát használja. Nekünk fontosak az ügyfelek így nálunk az a fontos, hogy megfelelően és rugalmasan tudjon alkalmazkodni a hálózat az ügyfeleink kérésére. A cégünk mára már szerencsére több különböző országba is jelen van így külföldi ügyfeleink is nőttek ezáltal több új dolgot tudunk behozni országunkba az újabb és újabb ismereteink miatt.

Cégünk kapott egy megbízást a Szász Tamás István Korháztól, hogy tervezzük meg, hozzuk létre és üzemeltessük a kórház hálózatát. A legelején észrevettük, hogy több területre kell bontanunk a hálózatot a könnyebb kezelhetőség miatt és azért, hogy a felhasználók megfelelően tudják használni a hálózatot. 6 területre osztottuk a hálózatot.

A kék színnel jelölt terület a kórház igazgatóság területe ahol 30 ember számára kellett biztosítanunk egy zökkenőmentes hálózatot. Ezen a területen 2db 2911-es Forgalomirányító, 4db 2960-as Switch, találhatóak még nyomatók és számítógépek is. Ezen a telephelyen többféle protokollt alkalmaztunk.

Második rétegbeli redundáns megoldásként az STP-t(Spanning Tree Protcoll) alkalmaztuk ami megelőzi a hurkok és szórási viharok kialakulását(később kitérünk erre bővebben is). Alkalmaztunk port összefogást (Port Aggregation Protcol) amely segíti az EtherChannel kapcsolat automatikus létrehozását. (A későbbiekben erre is bővebben kitérünk)

A forgalomirányítókon SSH(Secure Shell) protokollt használtunk mely segítségével titkosított hálózati kapcsolattal tudunk bejelentkezni egy távoli gépre.

Kapcsolókon VTP alkalmaztunk mely automatizált vlan információ cserét biztosít

PORT-SECURITY a biztonság miatt hiszen az interfészek maximum 1 címet tanulhatnak meg így ismeretlen cím esetén eldobják a nem ismert címet, és logolják a „sértést”

DHCP SNOOPINGOT alkalmaztunk így csak az ismert interfészeknek oszt címet a DHCP

Jelszó titkosításként SECRET jelszavak és service password-encryption az erősebb titkosítás érdekében

SSH hogy tudjunk titkosított távoli hozzáférést biztosítani az adminnak

Kék területet a kollégám fogja bemutatni részletesen.

A kék területtel kapcsolatban előszőr a vlanokra térnék ki

A területen belül 4db vlant használtunk a Vlan 15 ami az Orvosi igazgatóságé a Vlan 8 ami a Gazdasági igazgatóságé és vlan 7 ami a Főigazgatóságé és a vlan 99 ami a natív vlan.

**VLAN**

A vlanok azaz a Virtual local Area Network egy második rétegbeli kapcsolón létrehozható virtuális helyi hálózat, aminek célja a szórási tartományok méretének csökkentése így megkönnyíti a kiszolgált szervezet céljait.

A vlanok létrehozása egyszerű

Megkérem kollegám, hogy mutassa meg a show vlan brief kimenetelét az S2-őn, ami megmutatja a kapcsolón lévő Vlanokat és azok interfaceit.

mint látható a switch mindegyik vlant tartalmazza, ebből a vlan 15höz van hozzárendelve a két port.

A vlanokat két féle képpen tudjuk interfacehez rendelni: switchport mode trunk, switchport mode access. Az accesst arra az interfacere rakjuk, amit szeretnénk, hogy abba a vlanba tartozzon a porton lévő hálózat például a vlan 15 az fa0/10, fa0/12 interfacen az S2-őn. A trunk portokat a switchek közötti interfacekre és a switch router közötti interfacere. A trönk kapcsolat létrehozásához a fizikai kapcsolat két végén lévő portokat azonos parancsokkal konfiguráljuk. A switchport mode trunk parancs kiadása után az port egy állandósult trönk módra vált, ami dinamikus egyeztetésbe kezd, hogy trönk kapcsolatot alakítson ki. A trönkhöz megadhatunk egy natív vlant. Ez lesz az a vlan ahol a switchek tagelt és tageletlen csomagokat fogadnak a trunk portokon keresztül.

**VTP**

A vlanok létrehozásának megkönnyítésére használtuk a VTP version 2t azaz a Vlan Trunking Protocolt ami a Cisco Switchek között automatikusan cserélik a Vlan konfigurációs információkat. A vtp-nek két módja van az un szerver és a kliens. Szerverből egynek kell lennie a hálózaton belül tőle fogják megkapni a vlan információkat a vtp adatbázisból a kliens switchek. A VTP működéséhez kell egy vtp domain ami nálunk a szaszkh.hu lett. Ezt az összes kapcsolón be kell állítani a működéshez. a show vtp status kiadásával láthatjuk a VTP domaint, verziót és módját kliens/szerver.

**PAGP**

Ezeken felül a switcheken használtunk portösszefogást mi a PAGP-t választottuk, ami a cisco saját fejlesztésű protokollja így tökéletesen működik a ciscos eszközeinkkel. Ez a protokoll Etherchannel kapcsolatokat hoz létre. 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 show etherchannel summary parancs kiadásával látható, hogy milyen etherchannellek lettek létrehozva a switchen Itt például az S2őn az 1es, ami az Fa0/1 és Fa0/6 portokat fogja össze és a 4es, ami a Fa0/2 és Fa0/7es portokat.

**Feszítőfa (Spanning Tree Protocol)**

Az STP egy második rétegbeli protokoll, ami csökkenti a redundanciát és megakadályozza a szórási vihart. A szórási viharok, azaz broadcast storm akkor alakul ki, ha sok szórásos keret kerül be a 2. rétegbeli hurokba így az egész sávszéllességet felemészti. A feszítőfa protokoll biztosítja, hogy elkerüljük a hurkokat. A protokoll két járható port közül az egyiket mindig zárva tartja, tartaléknak. Az így lezárt porton csak akkor enged forgalmat, ha az elsődleges útvonal meghibásodik. A lezárt portokat az STP BPDU (Bridge Protocol Data Unit) -keretek küldésére használja. Ezek a keretek portokról, címekről és költségekről tartalmaz információkat. Mi erre a célra a Rapid PVST+-t használtuk, ami a cisco által készített Feszítőfa protokoll. A Rapid PVST+ (Rapid Per-VLAN Spanning Tree Plus) úgy működik, hogy minden vlanon külön feszítőfát hoz létre. (show spanning tree) Ez lehetővé teszi, hogy egyes vlanokat továbbítson a port a többit pedig blockolja. Biztosítja a vlanok terheléselosztását több porton így elősegíti a hálózati erőforrások optimalizálását. Ezen felül állítottunk be Portfastot. A Portfast beállítása után a switchportot lezárt állapotról továbbító állapotba kapcsolja így elkerülve a figyelő és tanuló állapotokat. Ezzel a hozzáférési pontok elérik a hálozatot azonnal és nem kell kivárni a konvergálást minden egyes vlanon.

**SSH**

Emellett, SSH-t is használunk a területen, melyek segítségével egy titkosított hálózati kapcsolaton keresztül bejelentkezhetünk egy távoli eszközre és konfigurálhatjuk azt, fájlokat másolhatunk át és parancsokat adhatunk ki. A korház szempontjából ez azért fontos ugyanis, ha valami hibásan működik, a rendszergazda, akár otthonról is orvosolhatja a problémát.

**Port-Security**

Ezen a telephelyen alkalmaztunk portvédelmet, azonban ezt a továbbiakban fogom bemutatni, a zöld telephelyen, mivel beállításuk megegyezik.

A rózsaszín terület, az otthoni dolgozó telephelye. Feladata, a kórház hálózatának felügyelete, illetve monitorozása. A területen egy WRT300N típusú vezetéknélküli forgalomirányító, valamint egy laptop, egy telefon és egy nyomtató található.

A forgalomirányító DHCP-n keresztül oszt IP-címet a dolgozónak.

Az otthoni WiFi hálózatok védelme csakugyan fontos, mint a nagyobb vállalatoké. Ha egy otthoni dolgozó hálózatába hozzáférést szerez egy illetéktelen felhasználó, akkor akár a vállalatról is szerezhet információt, melynél az „áldozat” dolgozik. Annak érdekében, hogy ez ne történjen meg, a lehető legkorszerűbb titkosítási módszerrel titkosítottuk, a hálózatot.

Mivel a WEP, ÉS A WPA titkosítás mára már elavultak és könnyen sebezhetők, ezért a WPA2-PSK titkosítást alkalmaztuk, mely egy előre meghatározott egyedi jelszóval védi a hálózatot. Emellett fontos megadni, a titkosítás formátumát. A TKIP-el szemben, az AES erősebb titkosítást használ, így arra esett a választásunk

Az otthoni dolgozó biztonsága miatt az otthoni routeren több biztonsági beállítást is használtunk. Ilyen a MAC-cím szűrés. Fontos, hogy a hálózathoz csak a dolgozó saját eszközei férjenek hozzá. Ennek érdekében megadtuk az eszközök MAC címét a router MAC szűrő táblájába. Ezzel elérve, hogy csak azok a bizonyos eszközök csatlakozhatnak

Ezen kívül kikapcsoltuk az SSID broadcastet így a hálózat nem látható mivel a router nem küldi az elérhetőséget jelző csomagokat. Így a wifihez csak az SSID tudatában lehet hozzá csatlakozni

A zöld terület a kórház főépületét szimbolizálja. A területen az orvosok számára kiépített hálózat mellett, egy, a vendégeknek szóló vezeték nélküli hálózat is a megrendelés része volt.

Továbbá egy Access Point, a forgalomirányító által nyújtott DHCP segítségével, a várakozó betegek számára, ingyenes WiFi elérést biztosít.

A switcheken Portvédelmet, és VTP protokollt alkalmaztunk (LEHET BŐVÜL!)

A korábbiakban már részleteztem a VTP jellemzőit, így nem boncolgatnám tovább. A beállítása azonos, a kék telephelyével.

**Portvédelem**

Az olyan cégeknél, ahol fontos, hogy a bizalmas információk biztonságban legyenek, nélkülözhetetlen, a behatolások elleni védelem alkalmazása. A Port-Biztonság ez ellen nyújt védelmet úgy, hogy megvédi a hálózatot az ismeretlen MAC-címektől, illetve beállítástól fűggően még naplózza is a sértés időpontját és a sértő MAC-címét.

Cégünk a telephelyen portonként egy MAC-címre korlátozta a hozzáférést, azt az egy MAC-címet pedig "sticky" azaz a ragadós módszerrel rendeltük hozzá a porthoz. Ha sértés történik, akkor a restrict állapot lép életbe, amely a protect állapottal elentétben nem csak eldobja a keretet, hanem a naplót is bővíti a fentet említett információkkal.

Megkérném kollégámat, hogy szemléltesse az aktuális beállításokat.

(VAAGY BEMUTATHATJUK A DOKUMENTÁCIÓN KERESZTÜL)

A lila területen a kórház laborja látható. Itt vizsgálják a technikusok, labori dolgozók, a beküldött humán mintákat.

A telephelyen egy 2911-es forgalomirányító, egy 2960-as switch, számítógépek és nyomtatók találhatók.

A végeszközök IPv4-es és IPv6-os címeket is kapnak, melynek a legrelevánsabb előnye a fokozott redundancia: Ha az egyik kiesik (IPv6 vagy IPv4) a másikkal továbbra is biztosítja a kapcsolatot.

Hogy IPv6-os és IPv4-es címek tökéletes kommunikációt biztosítsanak a többi hálózattal, OSPFv3 protokollt is szükséges volt bekonfigurálni a telephelyen.

Ha az IPv4-es kapcsolat megszakadna, fontos, hogy legyen olyan hálózat, amivel a LABOR kommunikálni tud. Ennek érdekében A LABOR és az IGAZGATÓSÁG között, üzemel, egy GRE alagút, ami továbbítja az IPv6-os címeket IPv4-es címeken keresztül az IGAZGATÓSÁG felé.

A GRE alagút egy ún. virtuális csatorna, amely összeköt két hálózatot. Az alagút keresztül megy az ISP-n(interneten), de kommunikálni csak a két érintett hálózat tud az alagúton keresztül.  
**<GRE szemléltetése PNETLAB-ban>**

A sárga telephelyen a kórház gyógyszertárának és a gyógyszerraktárnak hálózata látható.

A területen 2 darab 2911-es forgalomirányító és 2 darab 2960-as, számítógépek, valamint egy felhőszolgáltatás alapú adatbázis látható.

Ahhoz, hogy a sárga terület két forgalomirányítója közötti kommunikáció biztonságos legyen, PPP-t, azaz Pont-Pont protokollt alkalmaztunk. A PPP hibamentes adatátvitelt biztosít.

Hitelesíti a csatlakozó eszközt, ezzel megakadályozva a jogosulatlan hozzáférést. A PPP kétféle hítelesítési módszert használ. Biztonságtechnikai okokból a CHAP előnyösebb választás, ugyanis amíg a PAP a hítelesítés után, nem végez ismétlődő azonosítást, a CHAP igen.

A területen található egy Zóna alapú tűzfal, melynek köszönhetően a hálózatból csak HTTP és HTTPS csomagokat tudnak kiküldeni a dolgozók.

ZPF

A ZPF azaz Zone-Based Policy Firewall egy hálózat biztonsági megoldás, amit arra használtunk, hogy különböző biztonsági zónákra osszuk a telephelyet. Cégünk két zónát hozott létre a PRIVATE ami a belső hálózat és a PUBLIC ami a külső hálózat. Ennek célja a hálózat megvédése a jogosulatlan hozzáféréstől. A ZPF szabályokkal szűri a hálózatot. A korház esetében ez a szabály a PRIV-PUB policy, ami kiengedi a http, https, dns csomagokat a külső területre. Ennek demostrálására megkérném kollegám, hogy pingeljen a sárga területről kifelé. Mint látható a ping sikertelen viszont, ha egy weboldalt próbálunk elérni az problémamentesen sikerülni fog. A show policy-map type inspect zone-pair sessions parancssal láthatjuk az átvizsgált csomagokat és annak protokollját. (mint látható…). A show zone security parancs kiadásával láthatóak a zónák és azon belül a zónákba tartozó interfészek. A show zone-pair security vel láthatóak a forrás és a cél zóna.

Szürke területen található a korház szervertelepe. Itt található 1db Windows GUI PDC AD DHCP szerver, 1 Windows CORE BDC DHCP Failover szerver, Linux File, Web, Print szerver és egy Linux MYSQL adatbázis szerver. A területen található még 2db 2911-es forgalomirányító és egy 2960-as Switch. A forgalomirányitókon állítottunk be HSRP-t és Statikus NAT-ot.

**NAT**

A NAT fő célja a privát ipv4-es címek publikus címre fordítása. Cégünk a Statikus NAT-ot használt a szervertelep elérése érdekében. Nat lefordítja a belső ip címet, ami jelen esetben a szerverek belső címét fordítja külső ip címére, ezzel növelve a biztonságot mivel nem jut ki az internetre a belső ip cím A nat működését ugy tudjuk letesztelni, hogy megpingeljük a fordított ip-t <ping 89.89.89.89 kék hálózat gépéről>. Elsőre nem fog sikerülni a ping mivel a routernek meg kell keresnie a NAT táblájában az ip-címet majd lefordítani

**HSRP**

Annak érdekében, hogy a hálózat teljes mértékben hibatűrő legyen, az aktív forgalomirányító (SZERVER\_R) mellé lehelyeztünk, egy másodlagos forgalomirányítót (SZERVER\_BACKUP), azaz egy StandBy routert. Ez a folyamat a HSRP, azaz a Hot Standby Router Protocol segítségével működik.

A HSRP egy protokoll, mely segítségével kijelölhetünk egy routert, mely elvégzi a csomagok továbbítását, ezt nevezzük aktív routernek, és egy másik routert, amely szükség esetén (pl leáll az aktív router) átveszi az aktív forgalomirányító szerepkörét, azaz a csomagok továbbítását

A HSRP beállítása során meg kell adnunk egy ún. virtuális IP címet, mivel a végeszközök (pc, számítógép, stb...) Ezen az ip címen keresztül fogják elérni a továbbiakban a hálózatot. Az aktuális hálózatban ez az ip cím, a 192.168.100.126

Emellet fontos beállíti a prioritást, ezzel megadva, hogy melyik lesz az aktív, illetve a standby router. A kisebb prioritású router élvezi az aktivitást.

A konfigurációban látható egy ún. preemption beállítás. A preempt parancsot az aktív routerre érdemes kiadni ugyanis, ha hiba esetén leáll, akkor átveszi a standby router az aktív szerepkörét és amint újraindul, visszaveszi azt.

A szürke területen, 4 fontos szerepet ellátó szerver található.

A szervereket a Virtualbox nevű szimulációs programmal fogjuk bemutatni.

Mielőtt rátérnék a szerverekre, fontos kiemelnem a szimuláció kulcsfontosságú

Operációs rendszerét, a Mikrotik Router.

A mikrotik router egy ún. virtuális router, mely lehetővé teszi a hálózati

funkciók tesztelését anélkül, hogy fizikai hardvert kellene alkalmaznunk.

A routernek a valós környezetnek megfelelő IP címeket állítottuk be.

<ip/address/print>

A tűzfalbeállítások elvégzése elengedhetetlen a konfigurálás során.

Alkalmazásukkal A virtuális környezetet kívülről, a Host gépről is kezelni tudjuk. Ezen feladat lebonyolítására a Putty - nevű szoftvert használtuk.

Az <ip/firewall/nat/print> parancs kiadásával láthatjuk is a tűzfalbeállításokat.

Kollegám részletesen kitér a szerverekre.

Az első szerver, egy GUI felületű windows szerver, melyen üzemel a PDC, az AD, a DNS, és a DHCP

A PDC, Elsődleges tartományvezérlőt jelent. Ennek feladata a tartományon belüli authentikáció és authorizáció.

Az AD, egy ún. könyvtárszolgáltatás, melynek segítségével kezelni tudjuk, a "hálózati erőforrásokat" (mint például a felhasználókat, számítógépeket).

Az AD-ban létrehozhatunk különböző objektumokat. Ezek lehetnek felhasználók, vagy számítógépek akár. Ezen objektumok csoportosítására szervezeti egységeket használtunk. Az AD-ban 3 szervezeti egység található. Az első szervezeti egységhez, az igazgatósági tagokat, a másodikhoz a rendszergazdákat, a harmadikhoz pedig az orvosokat rendeltük. A felhasználók belépési joga, a munkaidő lejárta után, nem engedélyezett, ezzel is növelve a biztonságot.

DNS Legfontosabb funkciója, hogy az emberek számára érthető tartományneveket a hálózati eszközök számára értelmezhető IP-Címekre fordítja le, melyek segítségével ezeket az eszközöket meg lehet találni és címezni a hálózaton.

A DNS-en ún. Zónabeállításokat végezhetünk el. Ez a két zóna a Forward- és a Reverse Lookup Zone.

A forward lookup zone egy olyan zóna, mely domain neveket fordít IP-Címekre. <kép>

A Reverse Lookup Zone pedig, az IP-címeket fordítja hosztnevekre.

<kép>

A Windows BDC szerver, egy ún. készenléti tartalék szerver.

Backup Domain Controllert, és DHCP Failovert üzemeltet, tehát ameddig a PDC szerver aktív, a BDC szervernek nincs feladata.

A Backup Domain Controller képes a felhasználók authentikálására, de a tartomány változásait csak a PDC képes rögzíteni

<kép

A DHCP Failovernek köszönhetően a PDC az összes DHCP információt továbbítja a BDC-nek aminek köszönhetően leállás esetén, a számítógépek... továbbra is kapnak IP-címet, így nem szakad meg a kapcsolat

<Get-DhcpServerv4Failover parancs/kép>

A kórház weboldalát, és a felhasználók munkájának könnyítéséért egy Debian alapú Linux szerver felel.

A szerver webszerver, file és printszerverként üzemel.

A szerver elérhetővé teszi a felhasználók számára, a tanúsítvánnyal ellátott weboldalakat.

<kép>

A printszerver lehetővé teszi a felhasználók számára ugyanazon nyomtató használatát anélkül, hogy közvetlen kapcsolatot kell létrehozniuk minden egyes nyomtató és számítógép között.

<kép>

A szerver, egy külön erre a célra létrehozott meghajtón, képes eltárolni a felhasználók által feltöltött fájlokat. A tartománybaléptetéskor minden dolgozó kap egy a saját nevével ellátott meghajtót, melyen rendelkezésére áll 500 megabájt tárhely. A fájlszerver és a windows szerver közötti kommunikáció a Samba nevű szolgáltatásnak köszönhetően működik.

ACL

ACL azaz az Access Control list célja a hálózati forgalom szabálíozása. Az ACl-ek meghatárózzák hogy mely forrás címeken férhetnek hozzá a cél IP-címen és portokhoz. Az ACL-eket két féle módon nevezhetjük el: Azonosítokkal és saját nevekkel. Az utóbbit nevesített ACl-nek nevezzük

Acl-ekből két főtípus van a Szabványos és a kiterjesztett.

A szabványos ac-ek egysezrűbbek de nem ideálisak nagyobb hálózatokhoz mivel csak forrás cím alapján szűr. Ezért cégünk a kiterjesztett ACL-t választotta. a kiterjseztett ACL-ek forrás és cél ip-cím alapjánis szűr vlamint portok, protokollok és a forgalom típusa alapján is tudnak szűrni íigy sokkal rugalmasabb mint a szabványos ACL. Cégünk a szerverek védelmére használta az ACL-eket. Kollegám megmutatja a szerver\_R routeren a <show access-lists> parancsot.(itt kéne egy pingelés h nem működik) Itt látható az ACL-ünk ami megtagadja az icmp csomagokat így a szervereket nem lehet pingelni ami segíti csökkenteni a terhelését. A többi protokol enegdélyezve van így a szerverek hibamentesen tudnak működni a dolgozók számára (itt meg kéne egy weboldal nyitás). A HSRP miatt két forgalomírányitó vezet az ISP-felé ezért a másik routeren is létre kellett hozni az ACL-t.

ASA

A piros területen található egy Cisco ASA azaz Adaptive Security Applience. Ez az eszköz egy "biztonságiőrként" működik a hálózat számára. Az ASA felügyeli a ki és bemnő csomagokat és közben végrehajtja a beállíott biztonsági irányelveket, így megvédve a hálózatot az illetéktelen hozzáféréstől.

Az ASA feltételkészletekkel azaz class-map-ekkel és azon belül feletételekkel policy-map-ekkel vizsgálj a hálózatot

Cégünk feltételkészletnek az alap csomagvizsgálatot adta meg ami az általános csomagokat szűri például: ftp, tftp, icmp, http.

A feltételkészlet beállítása után ezt hozzá kell rendelnünk egy policy-maphez amiben pontosabban megadjuk hogy a feltételkészletből melyik csomagokat szeretnénk vizsgálni

**OSPF**

Cégünk forgalomirányítás szempontjából egy megbízható, konvergens, skálázható protokollt akart használni, ezért az OSPF-re esett a döntésünk. Az OSPF egy kapcsolatállapot alapú forgalomirányító protokoll. Cégünk az OSPFv2 és OSPFv3 protokollját is alkalmaztuk forgalomirányítás céljából. 4 területünk van, ami OSPF-et használ. Van az area 0 ami a backbone területünk, itt vannak a routereink. Az area 1 a labor területe. Az area 2 a főépület területe. Az area 3 a gyógyszertár és raktár területe. < show router ospf >. Itt látható az összes hálózat ami ospf alatt található. Ipv6os címek forgalomirányítására OSPFv3at alkalmaztunk. <show ipv6 route ospf> . A biztonság érdekében MD5-ös hitelesítést alkalmaztunk. Egy router esetében az MD5 gyakran használatos a hálózati forgalom, például a BGP (Border Gateway Protocol) üzenetek hitelesítésére.