BUDAPESTI GAZDASÁGI EGYETEM

PÉNZÜGYI ÉS SZÁMVITELI KAR

SZAKDOLGOZAT

Rinhoffer Dániel
Nappali munkarend
Gazdaságinformatikus alapszak
Logisztikai informatikus specializáció

2020

BUDAPESTI GAZDASÁGI EGYETEM

PÉNZÜGYI ÉS SZÁMVITELI KAR

A szoftver definiált nagy kiterjedésű hálózat

Belső konzulens: Bendes László

Külső konzulens: Klima Gábor

Rinhoffer Dániel

Nappali munkarend

Gazdaságinformatikus alapszak

Logisztikai informatikus specializáció

Alulírott .....RINHOFFER DÁNIEL..... büntetőjogi felelősségem tudatában nyilatkozom, hogy a szakdolgozatomban foglalt tények és adatok a valóságnak megfelelnek, és az abban leírtak a saját, önálló munkám eredményei.

A szakdolgozatban felhasznált adatokat a szerzői jogvédelem figyelembevételével alkalmaztam.

Ezen szakdolgozat semmilyen része nem került felhasználásra korábban oktatási intézmény más képzésén diplomaszerzés során.

Tudomásul veszem, hogy a szakdolgozatomat az intézmény plágiumellenőrzésnek veti alá.

Budapest, 2020. év .....május..... hónap .....05..... nap

.....

hallgató aláírása

Rinhoffer Dániel s.k.

Tartalomjegyzék

1. Bevezetés

A szakdolgozatom témája, ahogy a cím is mutatja, a szoftver definiált nagy kiterjedésű hálózat (SDWAN – software defined wide area network). Ez egy olyan technológia, ami jelenleg is már éles környezetben bevált megoldás, ami alternatívát nyújt a tradicionális nagy kiterjedésű hálózatokra. Pozitív tulajdonságai ellenére még nem a legdominánsabb termék a piacon.

Ebben a dolgozatban kívánom bemutatni, hogy milyen előnyei és hátrányai vannak a tradicionális megoldáshoz képest, valamint nagy részét fogja képezni a működésének ismertetése is. Jelenleg a hálózat kiépítésben és üzemeltetésben dolgozó szakemberek jelentős részének is ismeretlen a téma, akiknek a jövőben az átképzésük kell, hogy szem előtt legyen, mind személyes, mind vállalati szempontokat nézve, mely egy újabb problémát vet fel. Láthatólag az újnak mondható technológia olyan szinten működik, hogy a jóslások alapján ez a megoldás a jövő, előbb-utóbb le fogja váltani a tradicionális hálózat fogalmát teljes mértékben.

A szakmai gyakorlatomat egy olyan informatikai cégnél végzem, ahol a pozíciómnak hála beleláthatok abba, hogyan zajlik a hálózat üzemeltetés egy, még a tradicionális megoldással kiépített környezetben, valamint hozzáférhetek a szoftver definiált hálózati környezetekhez is. A személyes motivációm ebben a szakdolgozatban, hogy ismertessem az új alternatívát, és magam is olyan ismereteket halmozzak fel, ami hasznos lesz a karrierem szempontjából a jövőben. Számomra izgalmas témát dolgozok fel, ami reményeim szerint az olvasóknak is figyelemfelkeltő hatással lesz. Egy új technológiának mindig esélye van, hogy felborítsa a piaci helyzetet, a gyártók berögződött pozícióját és versenyképességét, valamint a munkaerő piac telítettségét, képzettségét egy adott szakmában.

A szoftver definiált nagy kiterjedésű hálózat felépítésének és működésének bemutatása közben véleményt kívánok alkotni arról, hogy jelenleg mennyire előrehaladott a fejlettsége és hogy milyen esetleges bővítések és változtatások lehetnek szükségesek az tervezés, kiépítés és az üzemeltetés szempontjából, valamint vizsgálatot

végzek, mennyire könnyíti meg a vállalatok munkáját és hogy milyen esetben éri meg korszerűsíteni az infrastruktúrát.

Ahogy már említettem, összehasonlításra fognak kerülni különböző nagyobb gyártól, akik termékükként biztosítanak szoftver definiált nagy kiterjedésű hálózat megoldásokat. Többek között a kutatásban helyet kap a Cisco, Juniper, VMware, Versa és további cégek is.

Olyan szempontokat fogok megvizsgálni, mint például a fogyasztói modell megoldások, azaz a különböző gyártók termékei mennyire fogyaszthatók „szoftver, mint szolgáltatás" (SaaS – Software as a Service) modellben, valamint, hogy a gyártó mennyiben szolgáltat rendszer integrálást, vagy a vevőnek kell maga megoldania az integrálást.

Fontos megvizsgálni a felhőszolgáltatásokhoz való kapcsolódás módját, minőségét. A jelenlegi informatika fontos részék képezik, tehát a hálózatnak is támogatnia kell azok elérhetőségét.

Példák pontokba szedve:

- Felhőszolgáltatás migráció és felhasználhatóság
- Globális hálózat összefogó pont (több szolgáltató által biztosított vonal egy helyen való összesűrűsitése, mint belépő pont a gerinchálózatba)

Kihagyhatatlan szempont még, hogy a nagy kiterjedésű hálózatok kiépítésénél, a távoli irodák összeköttetésében prioritások lehetnek. Értve ez úgy, hogy a szolgáltatók különböző megoldásokat kínálnak különböző áron, mint például Internetes kapcsolat vagy többprotokollos címkekapcsolás (Multi-protocol Label Switching - MPLS). A költséghatékonyság érdekében az említett prioritásoknak köszönhetően változó mely irodák melyik megoldással kapcsolódnak a gerinchálózathoz, ezért a meg kell vizsgálni, hogy mely gyártó milyen megoldásokat nyújt a hibrid környezet megvalósításához.

Különböző biztonsági és applikáció biztosítási technikák alkalmazását is kell, hogy támogassák a gyártók, ebben is össze lesznek hasonlítva, valamint elemezve lesz egy nagyon fontos szempont, a skálázhatóság. Ez elengedhetetlen a mai, rohamosan fejlődő világban, ahol cégek robbanásszerű növekedést produkálhatnak, ami kihat a hálózat nagyságára. Minél fejlettebb megoldással állnak elő a gyártók, annál jobb pozíciót vehetnek fel a piacon.

A fent említett példákban, ami nem egy teljes lista, prioritást állítok fel, mely elemek mennyire fontosok egymáshoz képest. Véleményem szerint ez egy érdekes és összetett téma, amiben nagyrészt megtalálhatók nagyon jól működő tényezők, de a kidolgozás során, a vélemény alkotás részeként kritikát kívánok alkotni a kevésbé sikeres tulajdonságokról. Fontos kiemelni, hogy a vizsgálat során a különböző példákhoz és illusztrációkhoz nagyobb vállalati hálózati architektúra modelleket használok. Ezen belül a CISCO SD-WAN megoldásához van hozzáférésem, így ebből kerülnek ki gyakorlati példák.

2. A szoftver definiált nagy kiterjedésű hálózat bemutatása

2.1 A technológia kialakulása

A szoftver definiált nagy kiterjedésű hálózat (SD-WAN) ötletét és a kialakítását a rohamosan fejlődő informatika váltotta ki, legfőbbképpen a felhő alapú szolgáltatások széleskörű elterjedése és az Internet stabilitásának növekedése.

A tradicionális formula is képes kezelni azt az infrastruktúra változást, amit a felhő hozott magával, de nagy hátrányokkal. Ebbe beletartozik, hogy a szoftver definiált nagy kiterjedésű hálózat sokkal költséghatékonyabb, könnyebben menedzselhető és megbízhatóbb az applikációk zavartalan elérését tekintve.

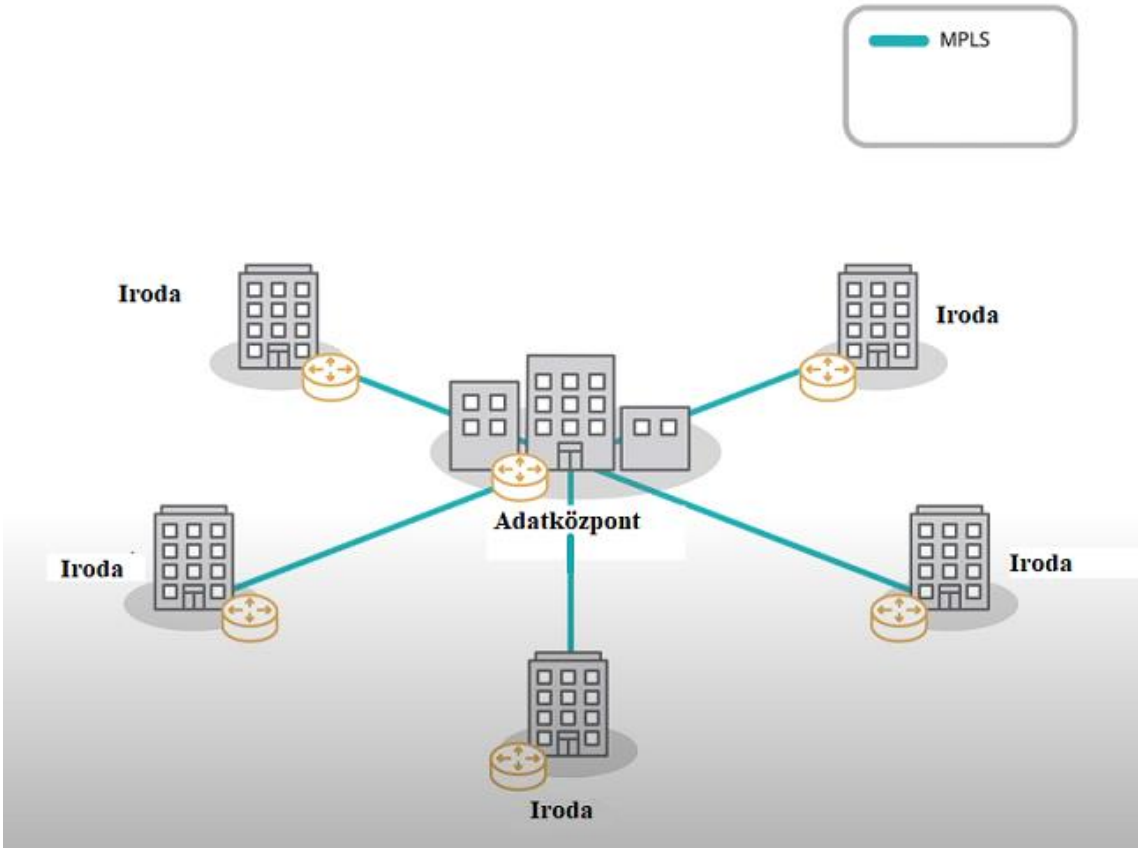
Ahhoz, hogy megértsük miért is bír ezekkel az előnyökkel, elsősorban az architektúrát kell összehasonlítani.

A tradicionális nagy kiterjedésű hálózat egy nagyobb vállalat számára általánosságban úgy néz ki, hogy a különböző irodák, ahol az alkalmazottak végzik a munkát, olyan alkalmazásokat és adatbázisokat használnak, ami a cég adatközpontjában (esetleg több adatközpontban, ez a vállalat globális terjeszkedésétől függ) vannak futtatva. Ebbe az adatközpontba csatlakoznak az irodák is, így tekinthetjük az adatközpontot forgalmi csomópontnak is. Mivel legfőbb esetben a cég számára kritikus fontosságú applikációkról beszélünk, mint például levelezés, könyvelés, fontos adatokat tároló adatbázisok, a kapcsolat megbízhatósága is egy kritikus pont. Az internet stabilitása a 2000-es évek elején nem volt elég megfelelő, így a szolgáltatók által kínált, stabil és gyors megoldást választották a vállalatok, a többprotokollos címkekapcsolást (Multi-protocol Label Switching - MPLS). Ez egy olyan forgalomtovábbítási technika, ami rövid útvonal címkéket használ hosszú hálózati címek helyett, így felgyorsítja a forgalom áramlását. Ez azonban a kiadások megemelkedésével járt, mivel ez a bérelt vonalak egy modern fajtája.

A következő ábrán szemléltemet, hogy is kell elképzelni ezt:

1.sz. ábra

Tradicionális WAN

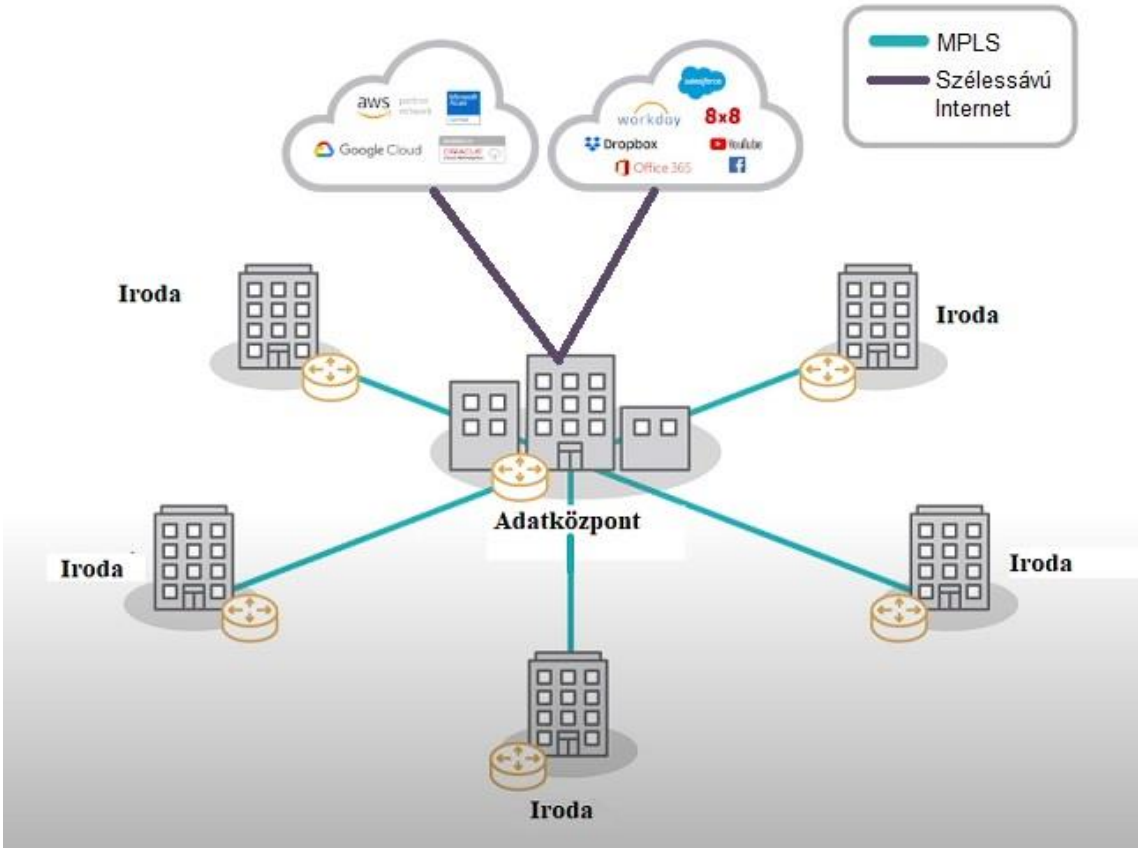


A felhő alapú szolgáltatások széleskörű elterjedésével az olyan nagyvállalatok, mint az Amazon, Microsoft, Google és egyéb cégek, saját, modern adatközpontokat hoztak létre azzal a céllal, hogy kedvező áron infrastruktúrát biztosítsanak különböző applikációk futtatására virtuális környezetben. Rugalmas megoldásaikkal és kedvező kínálataikkal elérték, hogy mára a legtöbb alkalmazást, amit a különböző cégek saját adatközpontjaikban üzemeltetett, átmozgassák a felhőbe. Ilyenek a már említett levelező, könyvelői, tárhelykezelő programok, mint például az Office 365, Dropbox, ahol magát a szoftvert, mint szolgáltatást kapják a vevők.

Az elérésük annyiban változott meg, hogy a felhő hálózatát összekötik a cég adatközpontjával egy bérelt vonalon keresztül vagy a mára szintén robbanásszerű fejlődést megélt szélessávú interneten keresztül.

2.sz ábra

Összeköttetés a felhővel



Ahogy az ábrán is látszódik, ez egy újabb problémát vet fel. Az adatforgalom, bárhol legyenek is az irodák földrajzi szempontból elhelyezve, fölöslegesen koncentrálódik a központi egységben. Ezzel nő a válaszidő két végpont között, ami ronthatja az applikáció használat minőségét, valamint még mindig a drága bérelt vonalak sávszélessége van használatban nagy mértékben.

Ezen hatások nyomására alakult ki a szoftver definiált nagy kiterjedésű hálózat, hogy kiküszöbölje ezeket a hátrányokat és a vállalatok hálózata alkalmazkodni tudjon a jelen informatikai fejlettségéhez.

2.2 Az SD-WAN működése

Az SD-WAN alap koncepciói közé tartoznak, hogy a nagy kiterjedésű hálózat központilag menedzselhető, egyszerűen skálázható, monitorozható, valamint nagymértékben automatizált legyen.

2.2.1 Központi menedzselés

A központi menedzselés ebben az esetben nem csak egy szimpla környezet, ahol a jól ismert technológiákat használva kialakítunk egy centralizált helyet, ahonnan minden elérhető. Az SD-WAN egy új módszerrel valósítja meg ezt.

A tradicionális nagy kiterjedésű hálózatban a forgalomirányítók több modulból tevődnek össze, melyeknek különböző feladatuk van.

3. sz ábra
Tradicionális CISCO forgalomirányító

A szemléltetés szempontjából az ábrán három részre választottam egy Cisco 7604-es modellű forgalomirányítót. Ez az eszköz tartalmaz egy vázat, amibe szabadon helyezhető vezérlő (Control Plane module) és be-/kimeneti modulokat (I/O module) lehet szerelni és ezeket a váz kapcsoló szerkezete köti össze, hogy kommunikálhassanak egymással.

A működésük végett fontos megemlíteni, hogy két féle csomagokkal kommunikál az eszköz, irányítási (routing packet) és irányított (routed packet). A különbség a kettő között, hogy az előbbi a vezérlő modult is érinti, míg a másik csak a be-/kimeneti modult. Az irányítási csomagok olyan információt tartalmaznak, amit különböző forgalomirányítási protokollok (példák a teljeség igénye nélkül: BGP, OSPF, EIGRP) felhasználásával egymással szomszédos eszközöknek küldenek a forgalomirányítók, tudatva a másikkal milyen kapcsolatokkal rendelkeznek és mit merre tudnak irányítani.

Ezeket az információkat a be-/kimeneti modul kapja meg a fizikai portokon az eszköz, majd továbbítja a vezérlő modulnak, ami egy adatbázist készít melyekben táblák vannak, amik alapján a forgalomirányítás történik. Ezt visszaküldi a be-/kimeneti modulnak a kapcsoló szerkezet segítségével, majd ezt használva az irányított csomagokat továbbítja a megfelelő helyre, avagy szomszédos eszközre a végpont irányába.

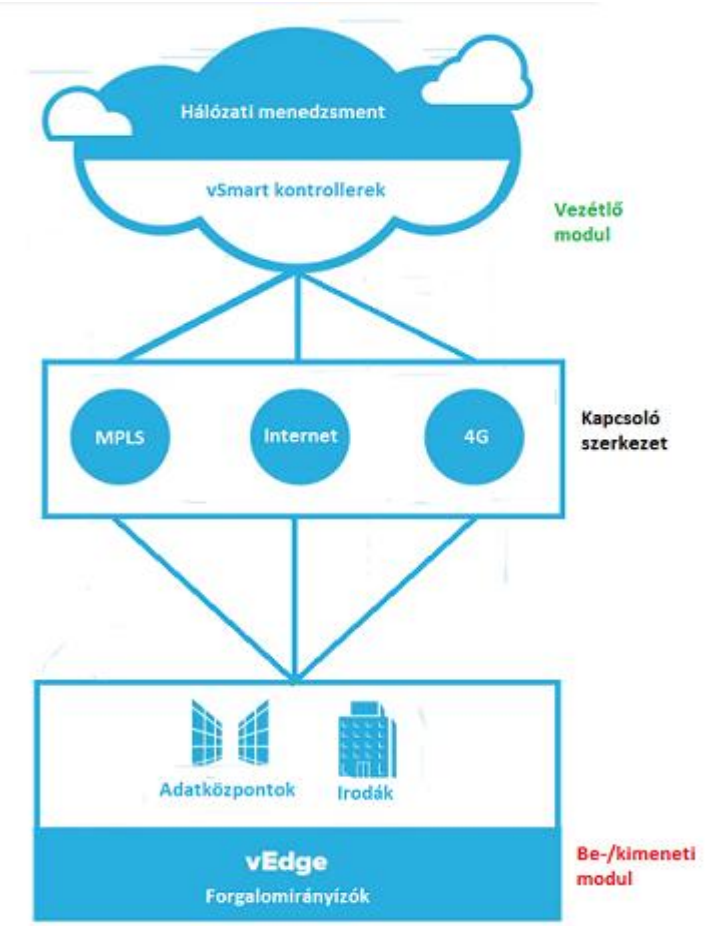
Ez röviden azt jelenti, hogy egy nagy hálózatnak, ami több száz, vagy akár több ezer forgalomirányítóval rendelkezik, minden adatot és frissítést egyenként kell feldolgoznia, valamint a változtatásokat külön be kell vinnünk az eszközökbe.

A szoftver definiált nagy kiterjedésű hálózat megoldása erre a különböző erőforrások átszervezése a forgalomirányítók struktúráját tekintve. A vezérlő modul teljesen központosítva van, a be-/kimeneti modul maradt fizikai vagy akár virtuális önálló modul és a kapcsoló szerkezet szerepét a hálózati vonal (például Internet, MPLS, 4G) veszi át.

Ezt az eredményezi, hogy az információ, amit eddig minden eszközben megtalálható vezérlő modul feldolgozott, egy helyre koncentrálódik, így ugyan az a formula egy jóval optimalizáltabb megoldásban érvényesül. Minden változtatást egy helyen kell véghez inni, azt az adott létesítmény perem eszközei (edge device) - ezek veszik át a hagyományos forgalomirányítók helyét, gyártótól eltérő az elnevezésük, például CISCO: vEdge, Silver Peak: EdgeConnect - egy hálózati vonalon keresztül megkapja és ez alapján operálnak tovább. Szemléltetés a 4. sz ábrán.

4.sz ábra

CISCO SD-WAN architektúra



2.2.2 Egyszerű skálázhatóság, automatizált környezet

Architektúráját tekintve az SD-WAN úgy lett megtervezve, hogy könnyebben és gyorsabban lehessen felállítani és bővíteni a hálózatot. Azzal, hogy a menedzsment központosítva és automatizálva lett, időt és erőforrást spórol meg a vállalat. A kiépítés először a hálózati menedzsment és a kontrollerek telepítésével kezdődik. Ez egy teljesen virtuális környezetben történik. A vásárló eldöntheti, hogy ez a rendszer a gyártó felhőjében, egy másik, felhő szolgáltatásokat nyújtó partner cégnél, vagy a vevő saját adatközpontjában legyen elhelyezve. Az utóbbi esetben a vevőnek biztosítania kell a megfelelő virtualizálható infrastruktúrát. Ezen felül van lehetőség választani, hogy a vevő saját maga építi fel a hálózatot vagy a gyártó segítségével, esetleg teljesen a gyártóra bízva.

Elengedhetetlen eleme a rendszernek egy úgy nevezett hálózati ”orchestrator” szerver. Egy 2015-ös Magyar Jövő Internet Konferencia címen kiadott tudományos cikk alapján szó szerint idézek:

„Jelenleg még nem alakult ki a megfelelő magyar terminológia az „orchestrator” elnevezés kiváltására, a felhő rendszer virtuális erőforrásainak koordinálását, a virtuális gépek menedzsment és vezérlési feladatait ellátó funkcionális elemet nevezik így.” (CINKLER TIBOR, SIMON CSABA, SZABÓ ÖRS, SZÉKELY SÁNDOR, JAKAB CSABA, 2015, p. 43 , https://www.hte.hu/documents/10180/1727937/HT_2016-1_MJIK2015_6_Cinkler_Simon_Szabo_Szekely_Jakab.pdf)

Továbbiaknak az „orchestrator” funkcióját („orchestration”) harmonizálásnak nevezik, így én is így fogok rá hivatkozni a szakdolgozatban.

A hálózati menedzsment felület kiépítése után a következő lépés a vezérlő felület kialakítása. Ez két részből tevődik össze, a kontrollerekből és a hálózati harmonizáló szerverből. Az utóbbinak az a szerepe az architektúrában, hogy a különböző elemeknek információt szolgáltasson, hogy kapcsolatok tudjanak létesíteni egymással. Ahhoz, hogy a vezérlő felület (amire a tradicionális nagy kiterjedésű hálózatban vezérlő modulként referáltam) életre keljen, a kontrollereket és a hálózati menedzsment felületet be kell konfigurálni. Ez után tudnak csatlakozni a harmonizáló szerverhez. Ezek lesznek az egyetlen tartós kapcsolatok a hálózatban DTLS (Datagram Transport Layer Security) protokollt használva, ami egy adatvédelmet biztosító protokoll publikus hálózatokon való kommunikálásra, mint például az Internet. Leginkább adat lehallgatás és adat befolyásolás ellen használatos.

Innentől kezdve már csak az irodák és adatközpontok helyi perem eszközeit kell a hálózathoz csatlakoztatni. Ezek az eszközök, amik ellátják a be-/kimeneti modul szerepét, amik relatíve skálázhatók a hálózatban, függően hány irodája, adatközpontja, kampusza van a világon a vállalatnak. A felhasználó szempontjából az egyetlen művelet, amit végre kell hajtani, az eszközök bekapcsolása és összekötése a helyi hálózattal (Local Area Network – LAN) és az Internettel. A folyamat automatikus, kiszállítás előtt a gyártó beprogramozza a perem eszközt, hogy amint kapcsolatot észlel, azonnal az adott harmonizáló szerverhez csatlakozzon. Tőle kapja meg az információt, hogyan csatlakozhat a kontrollerekhez, és amint ez megtörténik, felbontják a kommunikációt és létrejön a kapcsolat a kontrollerek és a helyi perem eszközök között is.

Mivel a harmonizáló szerver egy olyan szerepkört tud magának, amiben minden komponenssel kapcsolatban áll, így további funkciókat is ellát. Mint említettem a szoftver definiált nagy kiterjedésű hálózat kihasználja a fejlettebb szélessávú Internet adottságait, így a képbe jön a hálózati címfordítás. A vállalatok privát címzést használnak a belső hálózat kialakításakor és az Internet szolgáltatók biztosítanak publikus címeket azoknak. Ahhoz, hogy a kapcsolat működhessen, a privát és a publikus címek között fordítást kell alkalmazni. Csak a harmonizáló szervernek kötelező a publikus cím, így a hálózati címfordításhoz az adatok is itt koncentrálódnak és kerülnek kiküldésre a megfelelő eszközökhöz. Innentől kezdve képesek a perem eszközök és a kontrollerek virtuális privát csatornát kialakítani az Interneten és a hálózat működőképes. Ahhoz, hogy ezek a csatornák létre jöhessenek, egy hitelesítésnek is vége kell mennie.

A hitelesítés egy több lépésből álló folyamat. Először a kontrollerek és a hálózat menedzsmentnek (együttesen vezérlő környezet) kell hitelesítést végrehajtani a harmonizáló szerverrel. Első lépésben a harmonizáló szerver elküldi a vezérlő környezetnek a tanúsítvány hatóság által aláírt publikus tanúsítványát a vezérlő környezetnek és egy sorozatszám fájlt is. A harmonizáló szerver tárolja a hálózat eszközeinek sorozatszámát, hogy azok, amikor egymással kapcsolódnak, már ott legyen a saját adatbázisukban. A vezérlő környezet eszközei visszafejtik a tanúsítványból az organizáció nevét és ha ez megegyezik a sajátjaival, tudomásul veszik, hogy valószínűleg ez a megfelelő szerver, amihez csatlakozniuk kell, így a hitelesítés folytatódik tovább. Ellenkező esetben bontják a kapcsolatot. Utána megerősítik, hogy a tanúsítvány, amit kaptak, valóban a megfelelő tanúsítvány hatóság szerepel. Ellentétes irányban hasonlóan történik a folyamat. A harmonizáló szerver feloldja a titkosítást a kapott tanúsítványról, ellenőrzi a vezérlő környezet eszközeinek sorozatszámát, hogy megfelelőek-e.

A perem eszköz hitelesítési folyamata a harmonizáló szerverrel részben hasonló, mint a fent megfogalmazott, de vannak kulcsfontosságú eltérések. A szerver elküldi a tanúsítványát, amiből a perem eszköz ellenőrzi az organizáció nevet és az aláírást. Ez után a szerver egy úgy nevezett kihívás elé állítja a perem eszközt, egy 256 bit nagyságú véletlenszerű értékkel. Válaszul elküldi a sorozatszámát, a vázszámát, a tanúsítványát és a privát kulcsával titkosított 256 bit-es értéket. Az első két adat azért is fontos, mert a hálózat menedzsmentben a felhasználó manuálisan módosíthatja a listát az engedélyezett sorozatszámú perem eszközökről.

Amint a szerver megkapta a választ, ellenőrzi a sorozatszámot, feloldja a titkosítást a már megkapott publikus kulccsal és ellenőrzi, hogy megfelel e a 256 bit-es érték annak, amit ő előzőleg elküldött, végül ellenőrzi a tanúsítvány aláírását. Ezek a különbségek azért kellenek, mert ez első esetben teljesen virtuális környezetről beszélünk, ahol csak szoftvert kell hitelesíteni, az utóbbiban fizikai eszközöket, biztosítani kell az információt, hogy az adott sorozatszámú modul abban a vázban van, amiben lennie kell. A perem eszközök pedig ugyanazt a hitelesítést használják a vezérlő környezet eszközeivel, mint a harmonizáló szerverrel. Így tud a hálózatban minden entitás kommunikálni egymással biztonságos módon.

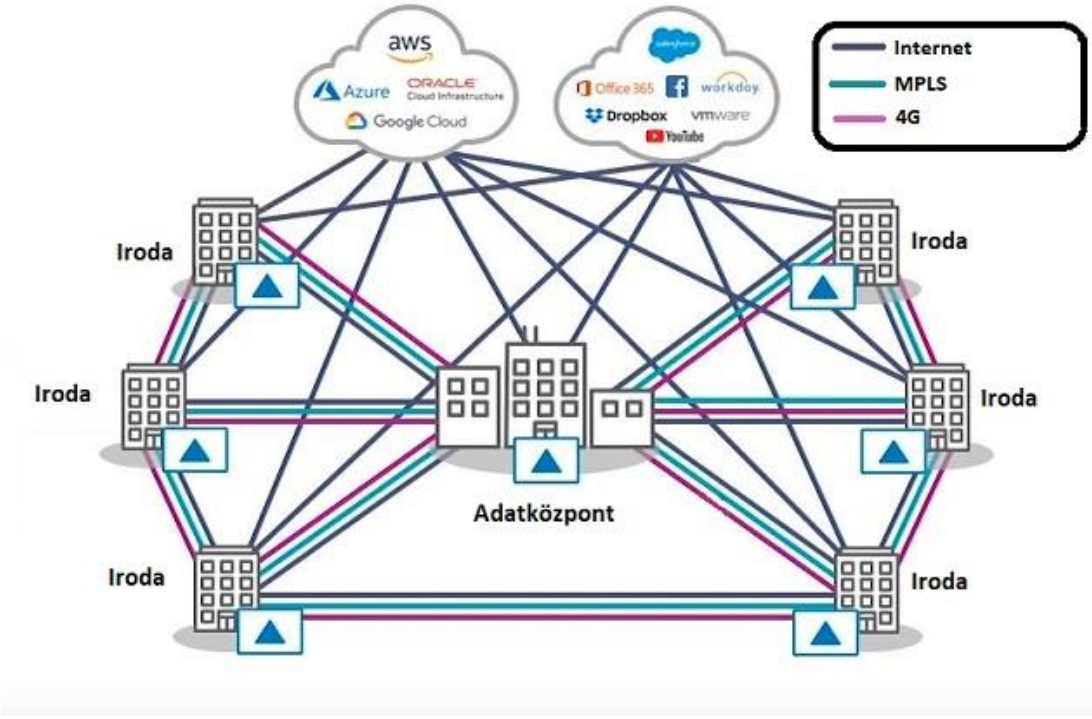
2.3 A hálózat személyre szabása

2.3.1 Topológia

A tradicionális nagy kiterjedésű hálózattal ellentétben, ahogy az első és a második számú ábrán is látható, a szoftver definiált megoldásban a topológia egy úgy nevezett virtuális teljes hálót (virtual full mesh) alkot.

5. sz ábra

Virtuális teljes háló topológia

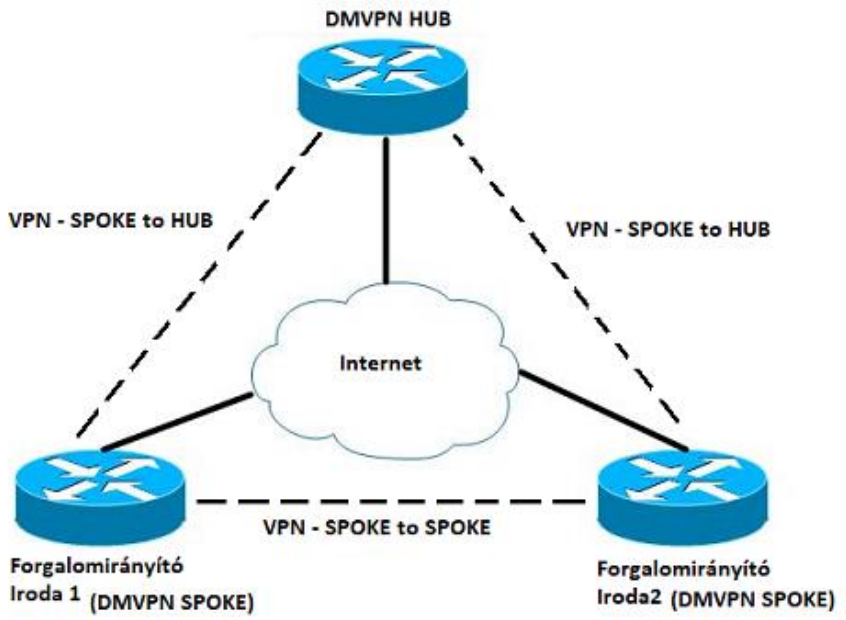


Az ábrán látható, hogy a technológia képes dinamikusan kezelni több fajta vonalat is, mint például a szélessávú Internet, bérelt vonalak (MPLS) vagy akár a vezeték nélküli 4G-t. Mivel a hálózat végpontjai legalább az egyikkel, vélhetőleg Internet kapcsolattal rendelkeznek így képesek közvetlen kommunikációt kiépíteni 2 iroda között ugyan abban a régióban, anélkül, hogy a távoli adatközpontot is meg kelljen járnia az adatforgalomnak.

Természetesen a tradicionális technológiában is van erre megoldás, a dinamikusan kiépülő többpontos virtuális privát hálózat (Dynamic Multipoint VPN – DMVPN). A lényege egyszerű, tartós kapcsolat építhessenek ki egy biztonságos virtuális csatornán (VPN) az Interneten keresztül az irodák egymás között, valamint az irodák az adatközpontokkal. Ideális esetben itt van elhelyezve a DMVPN HUB, ami a központi csomópontként szolgál. Minden forgalomirányító a HUB-hoz csatlakozik és innen kapják meg az információt is, hogyan tudnak egymáshoz csatlakozni. A hátrányai viszont az Interneten alapultak. Olyan szolgáltatások, amik érzékenyek a valós idejű késleltetésre, mint a hálózat alapú telefon (VoIP), a DMVPN nehezen felelt meg a vállalatok elvárásainak. Ezért sok esetben, ahol ezek fontos szolgáltatások a munkavégzéshez, maradtak az MPLS-nél és a DMVPN-t csak tartaléknak használták hiába magasabb költségekkel jár.

6. sz. ábra

DMVPN



Ahogy már említettem, az SD-WAN el tudja látni ugyan azt a funkciót, mint a DMVPN, viszont sok más szolgáltatást is nyújt ezen felül. Sokkal könnyebb konfigurálni a hálózatot, kevesebb idő alatt lehet felépíteni egy iroda kapcsolatát és tervezéskor nagy figyelmet fordítottak a hálózat teljesítményére, hogy a kritikus valós idejű szolgáltatások is zavartalanul futhassanak. Ezzel megalkotva egy alternatívát az MPLS-re. A felhőszolgáltatásokra való tekintettel a virtuális csatorna ugyan úgy kiépíthető az iroda és a szolgáltató között, nagyobb megbízhatósággal, mint a DMVPN megoldással.

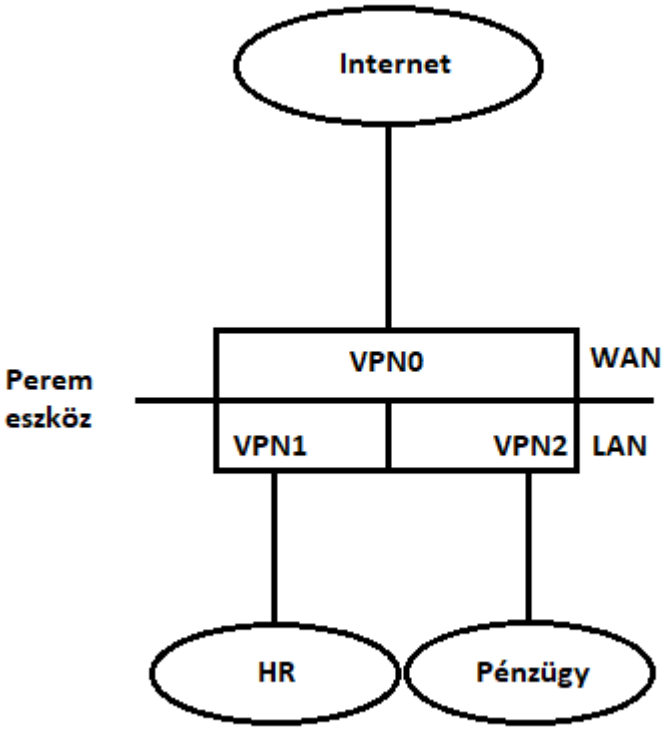
A topológia manipulálható úgy, hogy különböző szolgáltatások vagy vállalati szegmensek szerint szeparáljuk a kapcsolatot. Az irodákban különböző szervezeti egységek dolgozhatnak, mint például menedzsment, pénzügyi osztály, adminisztráció. Előfordulhat, hogy különböző csoportok különböző ügyfeleknek vannak dedikálva. Ilyen esetben elkerülendő, hogy a dolgozók hozzáférjenek számukra nem releváns bizalmas információhoz. Erre a megoldás a virtuális szeparáció. A hálózatokban a jól ismert virtuális helyi hálózatok (Virtual Local Area Network – VLAN) kialakítása a megoldás, de ezt a nagy kiterjedésű hálózatban is meg kell oldani. A tradicionális technológiákban a virtuális forgalomirányítás és továbbítás (Virtual Routing & Forwarding - VRF) fogalma valósítja meg. A módszer egyszerű, különböző forgalomirányítási táblák (routing table) egymástól elszeparálva léteznek egy eszközön belül.

Például egy vállalat a felhőben üzemeltet pénzüggyel kapcsolatos adatbázisokat és szolgáltatásokat egy ügyféléhez külön, amire van egy vállalati szegmense és az ide tartozó alkalmazottak a világ különböző részein lévő irodákban dolgoznak. Ahhoz, hogy más csapatok vagy szegmensek tagjai ne férhessenek hozzá a bizalmas adatokhoz, el kell választani az adatforgalmat. Külön eszközöket biztosítani ehhez drága megoldás, így kerül képbe a virtualizáció. Mivel a forgalomirányítási táblák adott eszközökön izolálva vannak, így mindenki csak azt tudja használni, amihez hozzáfér, lehetetlenné téve azt, hogy szabadon kommunikálhasson bármely végpontok akármelyik másikkal a hálózaton. Ehhez az is nélkülözhetetlen, hogy az útvonalon szereplő eszközökön mindenhol szerepeljen az adott azonosítóval rendelkező VRF.

A szoftver definiált nagy kiterjedésű hálózatban ugyan ez a megoldás szerepel más néven, például a CISCO Viptela VPN-nek nevezi.

7.sz ábra

CISCO VIPTELA VPN



A 7-es számú ábrán látható, hogy az irodák perem eszközei LAN és WAN szegmensekre vannak osztva. Ahogy korábban említettem, a LAN fel van osztva virtuálisan alhálózatokra (VLAN). Ezeknek az alhálózatoknak dedikálhatunk VPN címkét (VPN tag) a forgalomirányításhoz. Az alap VPN címke jelen példában a VPN0 kimondottan a nagy kiterjedésű hálózatra vonatkozik, ez felel azért, hogy az eszközök kapcsolatot létesítsenek egymással. Emiatt ez az összes eszközön szerepelni fog. A helyi alhálózatokhoz tartozó VPN címkék pedig a forgalom izolálásához tartozik. Magyarán a hálózatban az eszközök adott VPN-hez külön forgalomirányítási táblájuk lesz, mint a tradicionális VRF esetében. Például, ha Iroda1 pénzügyi részlege el szeretné érni Iroda2 pénzügyi részlegét, ahhoz az kell, hogy a perem eszközök behirdessék az útvonal adataikat a kontrollerek felé, amik eljuttatják ezeket a hálózat többi perem eszközéhez. Amint megvannak a szükséges információk, képesek kapcsolatot létesíteni egymással és kommunikálni azonos VPN-en belül.

Természetesen felmerül, hogy egy VPN-t egy megosztott szolgáltatásnak dedikálunk, például levelezés vagy adattárolás. Az, hogy minden szegmensnek külön szervert üzemeltessen a vállalat költséges és sok erőforrást igényel. Viszont a VPN-ek funkciójukat tekintve izoláltak. Erre a megoldás a tradicionális nagy kiterjedésű hálózatban is használt VRF szivárogtatás (VRF leaking). Több megoldás is van, statikusan és dinamikusan (a forgalomirányítási protokoll által) meghatározhatjuk a forgalomirányítókon, hogy melyik VRF-ben menjen tovább a forgalom.

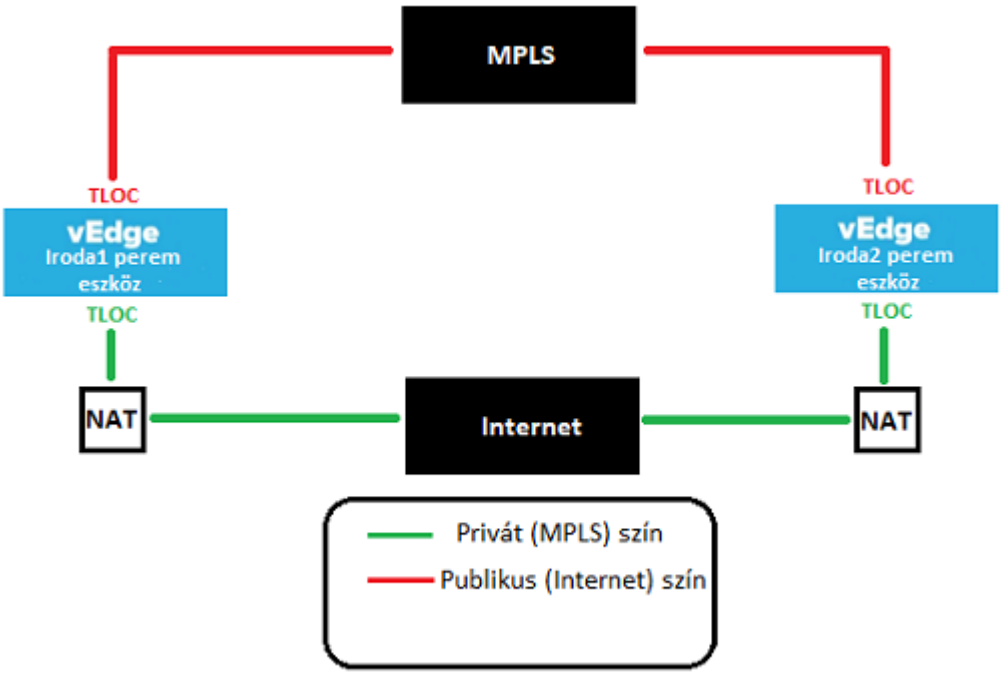
Az szoftver definiált nagy kiterjedésű hálózatban teljesen a kontroller látja el a szivárogtatás feladatát. Meghatározzuk, hogy VPN10 (ami példa kedvéért a megosztott levelező szolgáltatás) érdekelt abban, hogy hirdesse az útvonalait VPN1-nek, elérést biztosítva a HR-nek. Ha úgy döntünk, hogy a pénzügy nem érheti el ezt a szolgáltatást, egyszerűen nem engedélyezzük VPN10 és VPN2 közötti szivárogtatást, így teljesen izoláltak maradnak a hálózatban.

Egy másik fogalom is a képbe kerül amikor a VPN0-ról beszélünk. Ahogy már tisztáztam, itt találhatók meg azok az útvonal információk, amik kizárólag a nagy kiterjedésű hálózatra vonatkoznak. Az ide tartozó fogalom a CISCO által TLOC (transport location) névre keresztelt szállítási hely. Ez konkrétan a perem eszközök azon részre, ami egy szolgáltató által biztosított vonalhoz kapcsolódik (például Internet). A TLOC-nak vannak paraméterei, a fontosabbak: egy egyedi azonosító, beállított titkosítás a virtuális csatornához (például IPSEC) és egy szín. A szoftver definiált nagy kiterjedésű hálózat egyik újítása a színezés.

Egy irodához vagy adatközponthoz több szolgáltató által biztosított vonal is csatlakozhat, akár Internet, akár bérelt MPLS. Ahhoz, hogy ezeket azonosítani tudjuk, ki lett fejlesztve a TLOC harmadik paramétere, a szín. Két típusa van, privát és publikus (értve ezt a vonal típusára). Privát szín esetén jelöljük, hogy privát vonalról van szó, azaz nincs hálózati címfordítás használatban. Publikus szín esetén viszont következtethetünk arra, hogy hálózati címfordítás is közrejátszik a kapcsolat kialakítása közben. Ezek a virtuális privát hálózati csatornák (VPN tunnel) végpontjai.

8. sz ábra

Színezés



Az ábrával egy példát készítettem, hogyan nézhet ki egy színezés a publikus és a privát vonalakhoz. Az Internethez tartozik hálózati címfordítás (NAT), viszont az MPLS-hez nem. Ez azt eredményezi, hogy Iroda1 privát TLOC-ja nem tud kapcsolatot létesíteni Iroda2 publikusával, de hálózati szempontokból nem is szeretnénk, hogy próbálkozzanak. Ebben az esetben korlátozzuk egy beállítással, hogy azonos színekkel rendelkezők indítsanak kapcsolat kiépítést egymással.

Ezeknek az információkan a mozgását a hálózatban új forgalomirányítási protokollal oldják meg a gyártók. A szoftver definiált nagy kiterjedésű hálózat képes kezelni tradicionális, nem tulajdonban lévő forgalomirányitási protokollokat, azaz a technológia kompatibilis visszafele, de jelen esetben jellemző, hogy a gyártók saját megoldásaikhoz fejlesztenek új protokollokat.

2.3.2 Forgalomirányítási protokoll

A CISCO verziója a szoftver definiált nagy kiterjedésű hálózatához az Overlay Management Protocol (OMP) nevet kapta. Ez egy olyan mindenre kiterjedő kontroll protokoll, ami forgalomirányítási- és menedzsment információkat továbbít és választ el szabályokkal együtt a kontrollerek és a perem eszközök között. Sajátossága, hogy elválasztja a szolgáltatásokat a szállítástól. Az előző fejezetben említettek alapján egy szolgáltatás tartozhat egy bizonyos VPN doménbe azaz védve van, hogy látható legyen a VPN-en kívül. A tradicionális megoldásban kihívást jelent a domén és a szolgáltatás elérhetőségének bővítése. Az OMP könnyebb skálázhatóságot nyújt praktikusabb forgalom kezeléssel a TLOC-ok segítségével. Minden döntést a központosított kontrollerek végeznek el. A protokoll segítségével tanulják meg a kontrollerek a hálózat topológiáját és az elérhető szolgáltatásokat is.

Az OMP importálja a lokációk helyi hálózatainak forgalomirányítási információit az ott lévő tradicionális protokollok használatával (például OSPF, BGP) majd minden esetben továbbítja a kontrollerek felé. Ezeket az információkat a kontrollerek szabályozottan továbbítják a többi perem eszköznek. Mivel a protokoll egy rétegelt hálózati környezetben működik, azaz a vezérlés és az adat sík külön van választva, perem eszközök nem hirdetnek közvetlenül egymásnak forgalomirányítási információt. A kontrollerek és a perem eszközök egymással kizárólag vezérléssel kapcsolatos adatokat cserélnek.

Abban az esetben, ha valami probléma történik a kontrollerekkel és elérhetetlenné válnak, a hálózat működése nem áll le. A perem eszközök adat síkon tovább tudnak működni, a legutolsó használható információk alapján, amit a kontrollerektől kaptak. Ezt addig használják, amíg a hiba nem kerül elhárításra. A hálózati adminisztrátor ezzel időt nyer a kapcsolatok visszaállítására. Amint ez megtörténik a perem eszközök frissített hálózati információkkal tudnak tovább operálni.

2.3.3 Szabályozás

A gyártók a technológia kialakításakor nagy figyelmet szenteltek annak, hogy minél automatizáltabb legyen a hálózat. Kiépítéskor a hálózat felállása, bővítésnél a kapcsolat kialakulása és sok más téren a nulla beavatkozás elvét érvényesítik. A szabályok (informatikai nyelven „policy") létrehozása az, ahol a hálózat adminisztrátorai a legtöbb munkát végzik. Itt lehet definiálni megkötéseket, beállításokat, manipulálni a topológiát.

A tradicionális megoldásban minden beállítás külön-külön véghez kell vinni a forgalomirányítókon egy parancssoros felületen. Ez nehezen átlátható, sok munkával és sok odafigyeléssel jár. Egy apró hiba is nagy gondot tud okozni a hálózatban. Azonos gyártó különböző modellű eszközein akár ugyan azt a funkciót elvégő parancsok szintaktikája is különbözhet.

A szoftver definiált nagy kiterjedésű hálózati megoldásban a szabályokkal való konfigurálás centralizáltan történik a grafikus hálózati menedzsment felületen. Szabályozás alkalmazható biztonsági beállításokra, például szolgáltatásmegtagadással járó támadások (distributed denial-of-service – DDoS), titkosított adat lehallgatások és egyéb hálózati fenyegetések ellen. Továbbá optimalizálásra szolgáltatás minőség vagy drága vonalak kihasználása alapján. Meghatározható a topológia, mi mit érhet el.

A következő típusú szabályok alapvetően szerepelnek a hálózatokban:

- Kontroll szabály (Control Policy)
- Központosított adat kezelő szabály (Centralized Data Policy)
- Útvonal szabály (App-Route policy)
- Zóna alapú tűzfal szabály (Zone-Based-Firewall Policy)
- Minőség alapú szolgáltatás szabály (QoS policy)

Kontroll szabályokkal manipulálható a hálózati topológia. Fontos kiemelni, hogy az alapbeállítások egy teljes háló kialakítást adnak (full mesh), ami annyit tesz, hogy minden szabadon elérhet bármit a hálózatban. Például van egy adatközpont az Egyesült Államokban, három iroda Indiában és egy Angliában. Szeretnénk, hogy az indiai irodák tudjanak egymással és az adatközponttal kommunikálni, de az angliai irodát ne érjék el,

akkor ehhez egy kontroll szabályt kell létrehoznunk és abban korlátozni adott lokációk egymáshoz való kapcsolódását. Ugyanígy változtatható a teljes háló topológiáról a hálózat HUB-and-SPOKE megoldásra, ami egy centralizált hálózat (például 1.sz ábra).

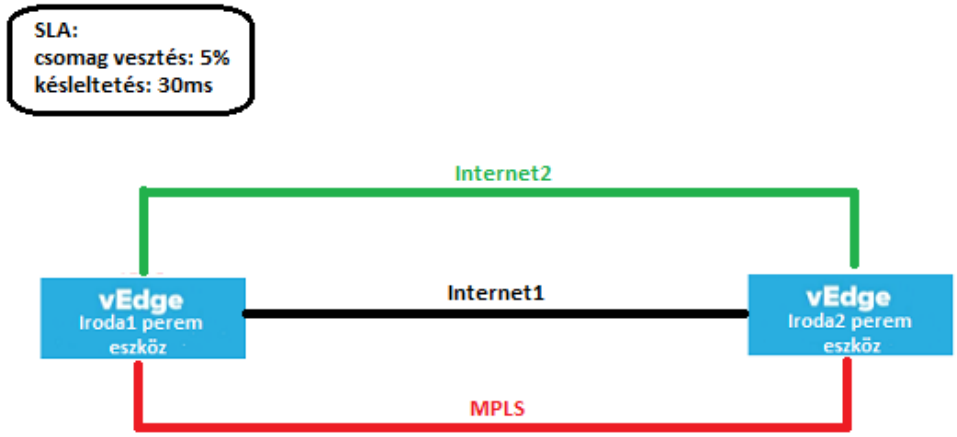
A szabályok logikailag egyszerűen működnek. Egyik részük a különböző összehasonlító feltételek, másik pedig egy művelet. Az előző példát tovább gondolva: Minden perem eszköz rendelkezik egyedi lokáció azonosítóval. Létre tudunk hozni egy olyan alapvető szabályt az indiai irodák csoportjára, hogy ha a kapcsolat kialakításakor az angliai iroda lokáció azonosítóját észleli, akkor végrehajtsa a műveletet, ami jelen esetben egy elutasítás lesz. Ugyan ez a logika átvihető szolgáltatásokra is, mint amikor az egy bizonyos VPN doménhez van társítva. A feltétel a VPN azonosító lesz, ha egyezés van, a művelet végrehajtható. A feltételek listája sokszínű, lehet TLOC-okkal vagy színekkel is operálni. Listákat lehet készíteni a lokációkra szabadon, például földrajzi vagy funkcionalitási szempontok alapján, majd a szabályokban ezekre a listákra lehet hivatkozni. A kontroll szabályok váltják fel a klasszikus értelemben vett route-map fogalmát, amik azonos funkciókat látnak el egy tradicionális nagy kiterjedésű hálózatban. Ez a típus a vezérlő síkon értelmezendő.

Az adat kezelő szabály ennél összetettebb. Itt olyan komplexebb szabályokat is alkothatunk, mint például a szolgáltatás láncolat (service chaining). Ez egy új sajátosság, amit a szoftver definiált nagy kiterjedésű hálózat hozott magával. A lényege, hogy automatizált adatáramlás legyen szolgáltatások között egy virtuális hálózatban. Olyan hálózati szolgáltatásokról beszélünk, mint tűzfal, titkosítás, terhelés kiegyenlítés, nagy kiterjedésű hálózat optimalizáció, de nincs limitálva hány kerülhet a láncba. A kontrollerek sok módon használhatják ezeket a láncokat, függően a forgalom forrásától, célpontjától vagy típusától. Ezen kívül a csomagok eltérően mehetnek át szolgáltatásokon, nincs kikötés, hogy egy láncban mindegyiket használni kell, valamint mivel virtuális környezetről beszélünk, a szolgáltatások könnyen mozgathatók. Hasonló a kontroll szabályhoz, viszont ez adat síkon értelmezendő, összetettebb dolgokat lehet véghez vinni.

Az útvonal szabállyal többek között optimalizálhatjuk a szolgáltatások minőségét. A vevők szerződés megkötésekor a szolgáltatóval megegyeznek bizonyos elvárási szintekben (ezt szolgáltatási szint szerződésnek hívják, azaz Service Level Agreement – SLA). Hálózati viszonylatban ez a vonal minőségére vonatkozik, például meghatároznak egy bizonyos maximum mennyiségű csomagvesztést, késleltesési időt.

Például a maximum csomagvesztés 5% és a legnagyobb válaszidő 30ms lehet. Ezt az SLA-t alkalmazzuk egy szabályon belül két iroda perem eszköze között.

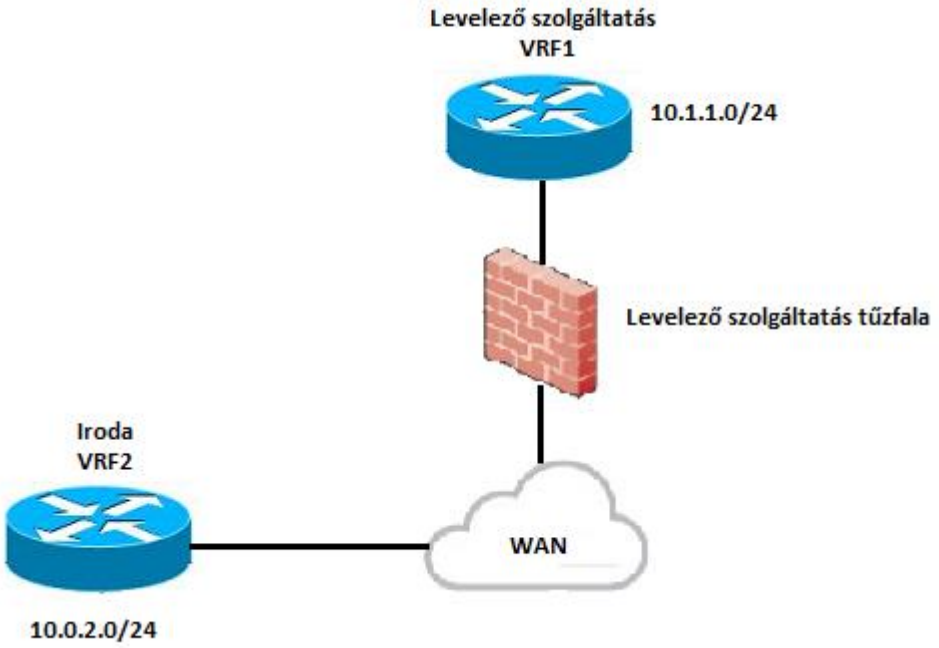
9. sz ábra
SLA



Ahogy az ábrán szemléltetem, a két iroda három vonalon keresztül tud csatlakozni egymáshoz. Prioritást szabhatunk szabállyal, hogy mikor melyik vonalat használja egy színlistából. Definiáljuk, hogy elsősorban Internet1-en menjen a kommunikáció, viszont folyamatosan vizsgálja a minőségét. Ha az SLA határain kívülre esik, váltson át Internet2-re. Amennyiben az se nyújtja az elvárt minőséget, csak abban az esetben használja a megbízhatóbb MPLS-t. Legtöbb esetben az MPLS-ért csak forgalomra számláz a szolgáltató, így költséghatékonyabb a hálózat is. Ez teljesen automatikusan nyújtja a legjobb adatátviteli minőséget szolgáltatásokhoz, végpontok közötti kommunikációhoz.

A zóna alapú tűzfal szabályok egy a szoftver definiált nagy kiterjedésű hálózat újítása. Tradicionális értelemben legtöbb esetben egy csomagszűrő tűzfalat használnánk arra, hogy kontrolláljuk adott források milyen célt érhetnek el.

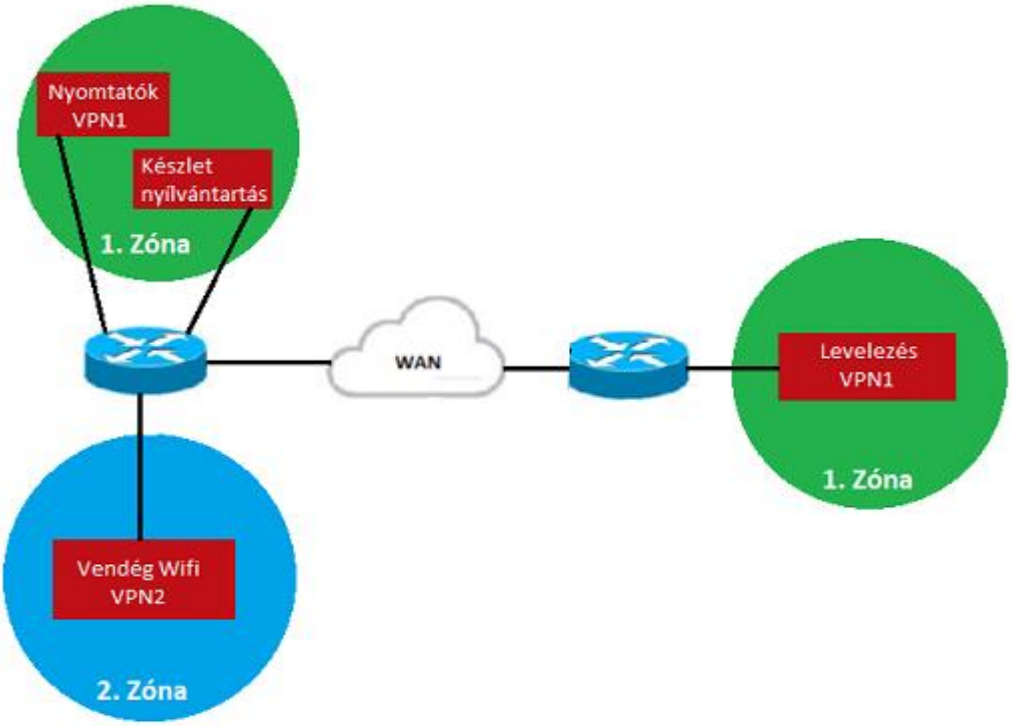
10.sz ábra
Tradicionális tűzfal



Az ábra szemlélteti, hogy egy iroda, ami különböző VRF-ben van, mint a levelező szolgáltatás, el szeretné érni a levelező szervert. Ilyenkor egy kliens végpont (tegyük fel számítógép) kapcsolatot kezdeményez. Ebben az esetben a kliens lesz a forrása a kapcsolatnak és a levelező lesz a végpontja. Útközben a forgalom áthalad a tűzfalon, ami megvizsgája azt. A hálózat adminisztrátornak fel kell vinnie a tűzfalra, hogy az iroda alhálózata és a levelező alhálózata között engedélyezze a kapcsolatot a 25-ös SMTP TCP port-on keresztül. Ellenkező esetben eldobja a csomagokat. A port-ot természetesen az üzemeltető határozza meg, ez csak egy példa, ami gyakran előfordul gyakorlatban is. Ezzel biztosítva van, hogy csak adott források bizonyos portokon érhessék el a szolgáltatást, más nem. Mivel külön VRF-ben van a két végpont, így alkalmazni kell egy VRF szivárogtatást is. Erre a tűzfal egy alkalmas eszköz, képes a statikus módszerrel végre hajtani a feladatot. Egyszerűen az egyik interfésze a VRF2-ben van, a másik, ahol a forgalom távozik a levelező fele pedig a VRF1-ben.

A szoftver definiált nagy kiterjedésű hálózat ugyanezt a módszert szabályokkal képes kezelni.

11. sz ábra
Zóna alap tűzfal szabály



Ezek a szabályok megelőzik azt, hogy nagyon hosszú adat kezelő vagy hozzáférési listákat (access-list – ACL) kelljen létrehozni. Fontos, hogy a szabályok egyirányúak a kapcsolatra való tekintettel, így mindkét irányba kezelni kell a kommunikációt. Az ábra segítségével egy gyakorlati példa, hogy a vendég wifinek engedélyezzük, hogy kapcsolatot kezdeményezzen a nyomtató szolgáltatással és figyeljük a vissza fele jövő forgalmat. Emellett tiltjuk a vendég Wifi-nek, hogy elérhessék a céges belső levelező szolgáltatást. Logikailag meghatározzuk, hogy a második zónában lévő vendég Wifi alhálózatából irányuló kommunikáció engedélyezve legyen az első zónában lévő nyomtató szolgáltatás alhálózata felé és a visszafele irányuló forgalmat pedig figyelje a tűzfal.

A nyomtatóknak viszont megtiltjuk, hogy bármilyen kommunikációt kezdeményezzenek a hálózaton, ez teljesen szükségtelen a szolgáltatás szempontjából, így leküzdünk egy biztonsági rést az által, hogy egy bárki által hozzáférhető publikus eszközt korlátozunk a hálózaton.

Hasonlóan a tradicionális megoldáshoz, a szabály összehasonlító feltételei lehetnek a forrás cím, forrás port, cél cím, cél port és a protokoll (például TCP vagy UDP). A művelet pedig átengedés, eldobás vagy figyelés. Fontos kiemelni, hogy ez egy állapot-nyilvántartó tűzfal megoldás, aminek a lényege, hogy nem csak egyszer vizsgálja meg a kapcsolat érvényességét és engedélyezi. Dinamikusan vizsgálja az átmenő TCP vagy UDP forgalmat attribútumok szerint, így, ha a kommunikáció közben veszélyes csomagokat észlel, mint például DDoS vagy Malware, azonnal kiválogatja és eldobja a kommunikációból.

A minőség alapú szolgáltatás szabály (QoS) első sorban arra szolgál, hogy prioritást szabjunk a forgalmaknak. Különböző szolgáltatások különböző hatásokra érzékenyek. Az FTP a késleltetésre kevésbé érzékeny, viszont a csomagvesztésre eléggé, valamint általában nagy sávszélességet igényel. A telnet és SSH érzékeny a késleltetésre és a csomagvesztésre, de nem igényel nagy sávszélességet. A VoIP és video szolgáltatások szinte mindenre érzékenyek, főleg a jitter-re ami a késleltetés váltakozását jelenti. Egy kihasznált hálózatban a forgalom elérheti azt az állapotot, amikor nem tud minden adat egyszerre gördülékenyen közlekedni. Értelemszerű, hogy meg kell szabnunk az említett tulajdonságok alapján egy prioritást a gördülékeny felhasználói élmény érdekében. Ez is egy több lépcsős szabály. Első sorban egy elérési lista (ACL) segítségével a szolgáltatásokat kategóriákba (Class) soroljuk. Létrehozunk és elnevezünk várakozási sorokat (Queue), és ezekhez társítjuk a különböző kategóriákat. Ezáltal definiáljuk, hogy melyik szolgálatás csoport melyik sorba tartozik amikor adatmozgásról van szó.

A harmadik lépés pedig, a várakozási sorok paraméterezése. Itt lehet beállítani olyan értékeket, mint sávszélesség és a buffer százalékos elosztása. Például megadjuk, hogy Queue1-be tartozó szolgálatások a VoIP, valamint a videó és ennek a várakozási sornak lefoglaljuk a sávszéleség 30%-át és a buffer 40%-át. Queue2-be pedig kerül a telnet és az SSH, ennek a sornak adunk 10% sávszélességet és 20% buffert. A maradék erőforrás pedig az alapértelmezett kategóriához fog tartozni, ide sorolhatók azok a szolgáltatások, amik az első lépésben nem illeszkedtek az ACL-ben megadott paraméterekhez.

Ezek a szabályok sok beavatkozást igényelnek, ezért itt merülhet fel a legtöbb emberi hiba is. Fontos tisztában lenni a hálózat logikai működésével. Például egy útvonal szabályban automatizáltuk, hogy a kapcsolat első sorban az Internet vonalon menjen és csak korában említett folyamatok hatására váltson át MPLS-re. E mellett van egy adat kezelő szabály érvényben, ami viszont kimondja, hogy MPLS TLOC legyen használatban. A csomagok először az útvonal szabályon mennek keresztül, majd pedig az adat kezelőn. Utóbbi felül írja az útvonal szabályt és így nem a kívánt beállítások fognak érvényesülni. Könnyen elfelejthető a szabályok sorrendje és elsőbbsége.

Hasonlóan egyszerű elrontani a hálózatot egy zóna alapú tűzfal szabállyal. Ahogy említettem, ez teljesen állapot-nyilvántartó tűzfal (stateful firewall) megoldás, aminél könnyen elvéthető az a hiba, hogy csak egy irányba engedélyezzük a forgalmat két zóna között. Ha az ellentétes irányra nem állítunk be műveletet (engedélyezés vagy figyelés), akkor el fogja dobni a csomagokat.

Harmadik példám, amit kiemelnék, az útválasztó szabályok létrehozásánál az SLA küszöb értékek definiálása. Rendesen fel kell mérni a környezetet, ahhoz, hogy meglehessen határozni milyen SLA-nak van értelme, ahelyett, hogy régi forrásokból nyert adatok alapján történjen a tervezés. SLA változhat applikációk között is. Ha túl alacsony vagy magas értéket állítunk be, nem érjük el azt a hatást, amit elvárunk a hálózatunktól. Vagy nem kapjuk meg a megfelelő minőséget, vagy nem lesz olyan költséghatékony a folyamat. Ha túl alacsony értéket határozunk meg, romolhat a szolgáltatás minősége, ha túl magasat, akkor pedig szükségtelenül sokszor vált át a rendszer a drágább MPLS vonalra. A QoS-t is ugyan ilyen precizitással kell beállítani, különben a rossz prioritás és elosztás rányomja a bélyegét a hálózat minőségére. Végeredményben rossz felhasználói élményt generál a szabály, holott ellentétes eredményt kívánunk elérni vele.

Más szemszögből a szabályokat két részre lehet osztani. Az egyik a centralizált szabályok. Ezeket a hálózati menedzsment felületen határozzuk meg, listával hivatkozva kikre lehet érvényes. Miután elkészültek, a hálózati menedzsmenttől eljutnak az információk a kontrollerekhez, majd továbbítják a megfelelő perem eszközökhöz. A másik rész a lokalizált szabályok. Ez a hálózati menedzsmenttől egyenesen a perem eszközhöz megy, ami akkor használatos, ha egy specifikus perem eszközre kell sajátos szabályt létrehozni.

A lokalizált szabályoknak két kategóriája van. A helyi kontroll szabály, aminek feladata, hogy manipulálja a helyi forgalomirányítási információkat. Ezek a perem eszköz mögötti szomszéd forgalomirányítótól származnak és tradicionális forgalomirányítási protokollt használnak, mint például OSPF vagy BGP. Ilyenek az SD-WAN környezeten kívül eső hálózati részek. Tekinthetjük úgy, hogy minden forgalomirányítási információ, ami a szoftver definiált nagy kiterjedésű hálózathoz tartozik, centralizált szabályban van definiálva és minden, ami tradicionális, az lokalizált kontroll szabályban. A második kategória a helyi adat szabály. Ennek szerepe, hogy adott perem eszközöknek speciális QoS-t vagy ACL-t lehet konfigurálni. Ez természetesen elvégezhető egy centralizált szabályban is, viszont, ha minden apró dolgot abban definiál a hálózati adminisztrátor, ezek a szabályok hatalmasra nőhetnek és nehezen lesznek csak követhetőek. Konfiguráláskor el kell dönteni, hogy melyik típus legyen érvényesítve, de logikusnak vehető, hogy a helyi adat szabályok nélkülözése nem tűnik a helyes döntésnek.

2.3.4 Felhő alapú szolgáltatások csatlakozása a szoftver definiált nagy kiterjedésű hálózathoz

Az előző fejezetekben esett szó arról, hogy a felhő alapú szolgáltatások, főleg a szoftver mint szolgáltatás (Software as a Service – SaaS) mennyire térhódító és fontos a jelenben. Ennek értelmében az SD-WAN is úgy lett kialakítva, hogy modernebb módon legyen megvalósítva a kapcsolat. Cél, hogy egyszerűen lehessen vizsgálni és kontrollálni a felhasználói élményt. Egyik legnépszerűbb példa erre az Office 365. Vállalatok nagy részre teljesen átszervezi a saját levelező rendszerét ebbe a felhő alapú szolgáltatásba. Mivel ilyen népszerű, a példáimat is ezzel fogom bemutatni, természetesen azok ugyan úgy érvényesek más szoftver szolgáltatásra.

A második számú ábrán látható, a tradicionális módszernél az a tendencia, hogy a felhő összeköttetésben van az adatközponttal és a felhasználók földrajzi elhelyezkedésüktől függetlenül azon keresztül érik el az applikációkat. Ezzel az adat fölöslegesen tesz meg nagy utat, növelve a forgalom körbeérésének idejét.

Az SD-WAN képes dinamikusan kihasználni az Internetet a leghatékonyabb módokon. Számos opció is felmerül, amikor egy iroda csatlakozik a felhőhöz. Többek között lehetőség van közvetlen Internet elérésre, regionális csomópontokon át, vagy a tradicionális formulát követve az adatközponton keresztül összeköttetést létrehozni. A kulcskérdés napjainkba, hogy melyik ezek közül az optimális. Ebben az SD-WAN erős megoldást biztosít. Lehetőség van valós időben mérni, kontrollálni és jelentést kapni az adott kapcsolatokról. A cél, hogy mint sok más tulajdonsága, ez is automatikusan, beavatkozás mentesen működhessen és csak egyszer kelljen jól felkonfigurálni.

A hálózati menedzsment felületen lehetőségünk van olyan külön applikációkra beállításokat végrehajtani, mint például a már említett Office 365. Ez azt jelenti, hogy külön felületet teremthetünk a szolgáltatáshoz tartozó kapcsolatok számontartására, kiértékelésére. A perem eszközökben egy beépített applikáció motor dolgozik, ami képes felismerni a felhasználó által kezdeményezett kommunikációt a csomagok vizsgálatával. Bonyolult applikációkról beszélünk, ezért a motor a begyűjtött információkat egy gyorsítótár táblába raktározza el, hogy a továbbiakban gyorsabban tudjon reagálni.

Technikailag úgy kell elképzelni, hogy első lépésben a vonalak teljesítményének mérése történik, eredménytől függően történik a választás, hogy melyiken menjen a forgalom. A mérésre nem a szokásos ICMP (Internet Control Message Protocol) ping szolgál, hanem egy HTTP vagy HTTPS ping, hiszen a kapcsolat is ezt a protokollt használja majd.

Alapvető értékek vannak figyelembe véve, mint csomagvesztés, csomag körbejárási idő és jitter. Ahhoz, hogy a rendszer ne reagáljon túl gyorsan, vagy túl lassan, a méréseket optimális időkeretekben kell elvégezni, mintavételezéshez hasonlóan. Az eredmények a központi menedzsment felületen nyomon követhetőek. Mielőtt a felhasználó bármit csinálna, már előre el van döntve a rendszer által, hogy melyik útvonalon tudja a legjobb feltételekkel elérni a szolgáltatást.

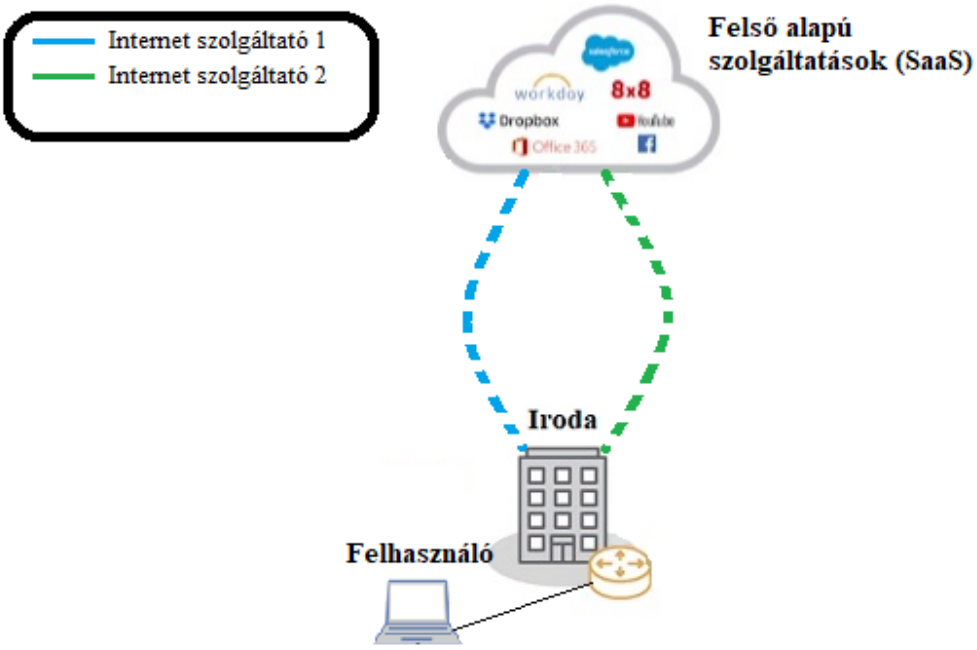
Második lépésben a felhasználó DNS név feloldást kérvényez egy adott SaaS applikációhoz. A perem eszköz felismerő motorja megvizsgálja a csomagokat. Ha nem felhővel kapcsolatosak, tovább irányítja a forgalomirányítási tábla alapján a megfelelő DNS szerverhez a vállalati adatközpontban. Ha viszont egyezést talál, az applikációt üzemeltető szolgáltató globális (és publikus) DNS szerveréhez küldi a kérést.

Harmadik lépésben épül ki a TCP kapcsolat. Ekkor készíti el az összehasonlító motor a gyorsítótár táblát (cache table) és tölti fel adatokkal. Ezek a végpont IP címe, port száma és a kimenő interfész. Így csökken a döntésekre fordított idő, szinte azonnali reakció megy végbe.

Példaként a gyakorlatban két igen közkedvelt megoldást szemléltetek:

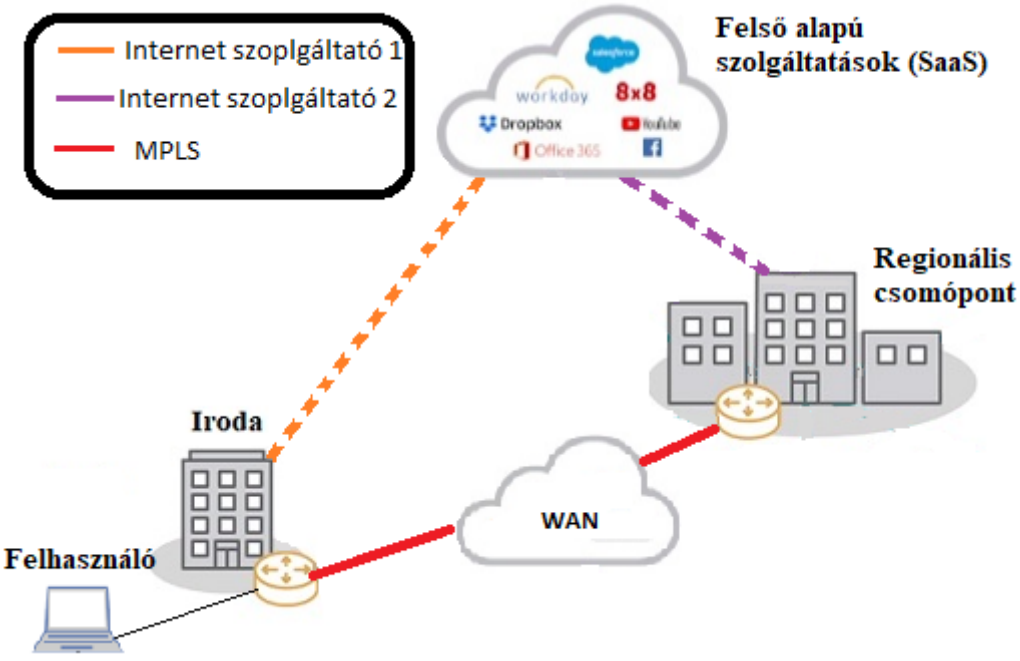
- Kettős közvetlen internet elérés (Dual Internet Access – DIA)
- Közvetlen internet elérés és regionális csomópont (DIA & Regional HUB)

12.sz ábra
Kettős közvetlen Internet elérés



Ebben az esetben 2 szeparált közvetlen Internet vonallal csatlakozik az iroda a felhő szolgáltatáshoz. Itt a már részletezett folyamatok érvényesülnek.

13.sz ábra
Közvetlen Internet- és regionális csomópont kapcsolat



A vállalatok szeretnek olyan megoldást is alkalmazni, hogy kialakítanak egy közvetlen Internet kapcsolatot a felhő szolgáltatás felé, valamint a redundancia érdekében összekötik az irodákat egy regionális csomóponttal (Regional HUB). Ez lehet MPLS vagy Internet is. A csomópontok általában földrajzilag kedvező helyen fekvő vállalati központok, nekik közvetlen Internet elérésük van a felhő szolgáltatáshoz. Itt kis mértékben különböznek a folyamatok a kettős közvetlen Internet eléréshez képest.

A két lehetséges útvonal vizsgálatakor figyelembe kell venni, hogy az egyik útvonalon az Iroda és a felhő között a vállalati nagy kiterjedésű hálózat is a kapcsolatba tartozik. Ez annyiban változtatja meg a vizsgálatot, hogy az iroda és a regionális csomópont kapcsolatát is kiértékeli a rendszer, a felhő és a csomópont kapcsolatával együtt. Ez az egész alkotja a második vonalat és kerül összehasonlításra a közvetlen Internet kapcsolattal. A csomópont és a felhő között a már említett HTTPS ping teszt fut. Az iroda és a csomópont között pedig két irányú továbbítás felismerés protokoll (Bidirectional Forwarding Detection – BDF).

Ez a protokoll is hasonló célokat szolgál, szomszédos eszközök között vizsgálja a csomagvesztést, csomag körbeérési időt és a jitter-t. Remek tulajdonsága, hogy rövid idő alatt észleli a hibákat, közel 1 másodperc a reakcióideje. A vizsgálat során a végpontok kontroll csomagokat küldenek egymásnak a megegyezett intervallumokban, hasonlóan a Hello csomagokat használó protokollokhoz.

Minden funkció, ami ebbe a fejezetbe tartozik, a felhasználói élmény magasfokú javítását teremti meg a tradicionális megoldáshoz képest, amikor egy felhő alapú szolgáltatásról beszélünk. Emellett egyszerűbb üzemeltetést biztosít a modern kezelő felülettel.

3. A piacon lévő főbb gyártók bemutatása

A piacon számos gyártó megtalálható amikor a szoftver definiált nagy kiterjedésű hálózati megoldásokat vesszük figyelembe. A technológia erőssége, hogy el lehet látni sok féle hálózati és teljesítmény javító funkcióval, miközben költséghatékonnyá lehet tenni az MPLS-el szemben. Sok megoldás létezik a piacok, a legnagyobb különbség az, hogy a gyártók mennyire képesek jól integrálni saját termékeiket és fejlesztéseiket a technológiába és hogy azok mennyire elégítik ki a vevők elvárásait. Természetesen a piacvezetők megoldásai általában komplexebbek és több funkciót is ellátnak, a kisebb gyártok viszont nagy hangsúlyt tudnak fektetni bizonyos aspektusokra, így el tudják nyerni az ügyfelek tetszését.

- **CISCO**

  A CISCO a múltban két SD-WAN gyártót is felvásárolt, 2012-ben a Meraki-t, 2017-ben a Viptela-t. Ennek eredménye, hogy két termékkel is jelen vannak a piacon.

  A Meraki előnyei kis- és közepes vállalatok hálózatánál jön ki leginkább, de képes nagyobb hálózatok kezelésére is. Támogatja a „csináld magad” (Do It Yourself – DIY) módszert, de ajánl menedzselést is. Egyszerű felhő alapú kontrollt biztosít, könnyű konfigurálás és üzemeltetéssel. A grafikus felülete úgy lett megtervezve, hogy végponttól végpontig egy kisebb informatikus csapat tudja menedzselni a hálózatot. Jól kezeli a kis eszközöket, mint például CCTV kamera, vagy hálózattal központosított órák. Közkedvelt választás, ha a vevő preferenciája az egyszerűség. Jelenleg a Meraki nem támogat komolyabb bonyolultabb szegmentációt. Helyi szegmenseket lehet létrehozni, mint például vendéghálózat, vagy demilitarizált zóna (DMZ).

  A Viptela ezzel szemben nagyobb, komplexebb nagy kiterjedésű hálózatokra van tervezve. A grafikus kezelő felülete úgy lett megalkotva, hogy egyszerű legyen használni, mégis támogassa a bonyolult szabályok, összetett műveletek végrehajtását sokkal részletesebben definiálással. Jól kezeli a kompatibilitás kérdését tradicionális hálózati elemekkel. Felhasználó barát kontrollt biztosít az OSI modell 4-7 rétegekhez is.

Az architektúrája az alapoktól úgy van felépítve, hogy komolyabb szegmentációt lehessen megtervezni és felépíteni. A már ismertetett VPN szegmentáció működése a Viptela sajátja. Különböző topológiák, forgalomirányítási- és biztonsági szabályokat lehet érvényesíteni a szegmensekre.

Mondható úgy is, hogy a CISCO két megoldást kínál különböző érdekeltségű ügyfeleknek a beépített funkcióik által. Természetesen, mivel egy gyártó alatt fut már mind a két megoldás, vannak közös előnyök és hátrányok is. Ilyenek például, hogy jól érvényesül a SaaS fogyasztási modell, a gyártó által történő menedzselés, de a DYI modell is könnyen alkalmazható. Erősen támogatják a hibrid környezeteket (Internet+MPLS+LTE). Jók a topológia kezelés, WAN optimalizáció, az automatizálás és hibáknak való ellenállás terén is, valamint kiválóan támogatja a 4G-t is. Hátrányai viszont abban jönnek elő, hogy bonyolultan működik a licenszelés DIY modell esetén.

- **Silver Peak**

  Megoldásuk jól képes kezelni az applikáció támogatást, felhasználói biztonságot és az intelligens adatáramlást. A cég inkább az Internet felé tolja el a preferenciát, ezzel előtérbe helyezve a költséghatékonyságot a drága privát vonalak kivezetésével a hálózatból. Kevésbé mondható egy kapcsolatokat szabadon támogató gyártónak. Tesztjeik azt mutatják, hogy sokkal kedvezőbb a terméküket szélessávú Interneten használni, mint tradicionális nagy kiterjedésű hálózatot üzemeltetni. Ez azoknak a cégeknek lehet kedvező, akiknek nincs, vagy csak nagyon kevés kritikus lokációjuk van. Ennek a rendszernek a működését segíti, hogy egy remek WAN optimalizáció van beépítve és olyan egyedi tulajdonságok, mint a továbbítási hiba kijavítás, aminek célja a hibás adattal rendelkező csomagok újra építése. A licenszelés jól működik előfizetés alapon minden komponensre. Kiváló a hálózat aggregálás terén.

  Hátrányai közé sorolható, hogy kevesebb biztonsági lehetőséget támogat azzal, hogy szűk integrálhatóságot enged más, jól ismert biztonsági szolgáltatásokat nyújtó gyártó technológiájához. A 4G támogatottsága se különösebben fejlett még.

- **Aryaka**

  A SmartCONNECT nevű terméküket kínálják az SD-WAN piacon. Stratégiájuk, hogy hibrid hálózatot kínálnak, kritikus forgalmat az MPLS gerinchálózatukon keresztül, ami kevésbé fontos, pedig Interneten keresztül továbbítják. Remek teljesítményt nyújt olyan cégeknek, akiknek az irodái földrajzi szempontból szétszórtan helyezkednek el. Jó WAN optimalizációs megoldásaik vannak és több SaaS útválasztóval is rendelkeznek, a felhő alapú szolgáltatások stabil elérését biztosítva. Leginkább a közepes cégeket célozzák meg a piacon, akiknek a céljuk, hogy minél jobban kiszervezzék a hálózat menedzselését. Komplex változtatásokhoz szükséges bevonni a támogató csapatukat. Előnyük, hogy gyors és stabil hálózatot biztosítanak a felhő szolgáltatások eléréséhez, menedzselik a hálózatot, viszont a korlátolt lehetőségeik a hátrányaik is. Stratégiájuknak köszönhetően a kis- és nagy vállalatoknak nem ideális a kínálatuk, valamint azoknak, akik maguk szeretnék kezelni a hálózatot.

- **VMware**

  A VMware egy meghatározó szereplő a piacon a velocloud nevű termékükkel. Sok tapasztalatuk van a multinacionális vállalatok kiszolgálásában. Hasonlóan a Silver Peak-hez, a velocloud-ban is megtalálható a továbbítási hiba kijavítás (FEC) és a TCP optimalizáció. Szolgáltatnak hardvert és szoftvert is teljes tűzfal funkcionalitással. Olyan cégeknek kedveznek igazán, akiknek szükséges a független szállítás egy biztonságos rétegben a publikus és a privát vonalak bármely kombinációján keresztül és biztonságos kapcsolatot várnak el a vállalati adatközpont és a SaaS applikációk között. Jó teljesítményt biztosítanak késleltetés érzékeny applikációknak (például VoIP és video) rosszabb minőségű vonalakon is. Folyamatosan bővítik az integrációs lehetőségeket az NSX platformjukra, aminek része a szoftver definiált hálózatuk (ide tartozik a szoftver definiált helyi hálózati megoldásuk is – SD-LAN). További előnyük, hogy a skálázhatóság határa nagyon magas, kompatibilisek tradicionális megoldásokkal és hasonlóan a CISCO-hoz, ha a kontrollerek elvesztik a kapcsolatot, a hálózat remekül képes tovább működni, amíg helyre nem állítják a rendszert. Hátrányai közé tartozik, hogy a FEC miatt kevés a támogatás a komolyabb WAN optimalizációra. Nincs támogatva kellően az eszköz programozhatósága, hogy a hálózati kapcsolók mérni tudják a hálózat teljesítményét.

Ez egy költség spóroló tulajdonság, hogy ne kelljen külön drága eszközöket venni erre a célra.

- **Versa**

  Ő egy olyan gyártó, akinek a terméke magas színvonalon képvisel a céget az SD-WAN piacon. a SaaS, a DIY és a menedzselt szolgáltatás fogyasztási modelljük is remek teljesítményt nyújt. Kiválóan támogatják a különböző WAN technológiákat, a virtualizálást.

  A megoldásuk elsők között van az analitikát tekintve. Jól támogatja az adatelemzést és bányászatot, ami fontos a hálózat bővítés megtervezésében. Jól használható jelentéseket tud készíteni a vonalak állapotáról, ami hasznos szabályok definiálásakor, főleg kontroll és adat szabályok terén. Támogatja harmadik fél által tervezett hálózat menedzsment szoftvereket is. Nem rég jelentették be a Titan elnevezésű felhő menedzselt SD-WAN megoldásukat. Ennek része a dinamikus applikáció prioritás állítás, automatikus terhelés elosztás a vonalak között, erősebb biztonsági szolgáltatások, mint például a malware szűrés és többek között megbízható vezeték nélküli kapcsolatok támogatása. A visszafele kompatibilitás kicsit elmarad pár gyártóhoz képest és a különböző SLA kezelés eltérő földrajzi viszonylatokhoz se a legkiemelkedőbb tulajdonság.

- **Juniper**

  A gyártó leginkább nagy vállalatok és szolgáltatók hálózatában van jelen. Viszonylag későn lépett be a piacra a többi nagy gyártóhoz képest. A WAN optimalizációjuk is kissé elmarad a versenytársakhoz képest. Nem rég adták ki legújabb fejlesztésüket, LAN funkcionalitást ötvöztek az SD-WAN mellé. A cég lépései a szoftver definiált hálózat jelenlegi helyzetére reflektálnak, miszerint a gyártók gyakran konkrét felhasználási esetekre koncentrálnak, nem pedig teljességre törekedő vállalati megoldást kínálnak. Emellett figyelmet fordítanak a vezeték nélküli hálózatokra. Mindegyik fogyasztási modellben jól szerepelnek, az említett fejlesztéssel a hibrid környezetet is jól kezelik.

- **Cato Networks**

  A gyártó terméke az SD-WAN piacon a Cato Cloud. Egy kisebb cégről van szó, ami biztonság orientált megoldást szolgáltat, ami előnyükre válik, mert a termékük minden aspektusába beágyazták a különböző védelmi tulajdonságokat. Remek teljesítményű nagy kiterjedésű hálózatot biztosít azzal, hogy a privát gerinchálózatukon keresztül továbbítják az ügyfél virtuális privát hálózatának forgalmát a kapcsolódási pontjaik között.

  Ez a megoldás leginkább közepes vállalatoknak előnyök, akiknek fontos szempont a védelem. Hátránya, hogy földrajzilag közel kell lenni valamely kapcsolódási pontjukhoz (Points of Presence – PoP). Nincs még nagy tapasztalatuk a nagyobb és komplexebb SD-WAN telepítésekben, amiket hagy vállalatok igényelnek.

- **Citrix**

  A Citrix nagyon ismert cég, a szoftveres virtualizációról terén. Ilyenek a virtuális asztali infrastruktúra megoldásai (Virtual Desktop Infrastructure – VDI) és a WAN optimalizációs termékei. Az SD-WAN piacára a NetScaler nevű termékükkel vannak jelen.

  A közelmúltban végzett biztonsági fejlesztéseknek köszönhetően nagy előrelépést értek el ezen a téren. A NetScaler-hez integráltak több terméket is, ezáltal közös interfészről lehet őket menedzselni. Példa erre a MAS (Management and Analytics System). Hátrányai a többi megoldáshoz képest a skálázhatóság mértéke, a vezeték nélküli hálózatok támogatása és az eszközök programozhatósága sincs a legmagasabb szinteken. Gyengébb támogatást ad a több bérlős kialakítást, ami olyan szoftverek és infrastruktúráknál kulcsfontosságú, amiket egyszerre több ügyfél is használna. Így ez a megoldás kevésbé vonzza be a menedzselt szolgáltatást biztosító cégeket.

  Rugalmasan szolgáltatnak fizikai és virtuális hardvereket is.

- **Riverbed**

  A Riverbed elsősorban nagy kiterjedésű hálózatok teljesítményének javítására fókuszáló cég. Az SD-WAN megoldások a termékei köré lettek integrálva. A SteelHead és SteelConnect ötvözetével vannak jelen a piacon. Az előbbi a platformjuk, az utóbbi a forgalomirányító technológiájuk a szoftver definiált nagy kiterjedésű hálózathoz. A többi gyártóhoz képest kissé elmaradottak biztonsági és hiba ellenállási funkciók tekintetében. Szolgáltatásuk virtualizálható AWS (Amazon Web Services) és Azure (Microsoft felhő) környezetekben is. Előnyeik a DIY és a menedzselt szolgáltatás fogyasztási modell, és az applikációk kezelését érintő tulajdonságok hálózati viszonylatban. Az újításaik, mint például a SaaS Accelerator, ami felhő szolgáltatásokhoz biztosít gyorsabb adatáramlást, modernebb szolgáltatás láncolás. Növelik a rugalmasságot és a biztonságot a multi-could hálózatok terén. Ezekkel és a jövőbeli fejlesztéseikkel potenciálisan pályázhat jobb helyre a gyártók listáján.

- **Fortinet**

  A korábban csak biztonsággal foglalkozó cég is belépett az SD-WAN piacra. a Cato Could-hoz hasonlóan itt is a biztonságot helyezik előtérbe. Termékük, a Fortinet Secure SD-WAN az utóbbi években a biztonságot leszámítva nem szerepelt olyan kimagaslóan, mint legnagyobb versenytársai. Ennek kezelésére a közelmúltban tett fejlesztések és megkötött partnerszerződések hatására a szakértők egyre jobban elismerik és kihívóként említik a piacvezetőkkel szemben. Ilyenek például a kis és közepes vállalatoknak kedvező vezeték nélküli hálózat támogatások, valamint az Equinix-el kötött partnerség. Párosították a Fortinet Secure SD-WAN-t a partner Network Edge megoldásába, hogy az ügyfelek dinamikusabb publikus felhő elérést kapjanak egy felszerelt SD-WAN megoldással, ami jó közepes és nagyvállalatoknak egyaránt. Törekednek arra, hogy csökkentsék a nagy kiterjedésű hálózat komplexitását és költségeit, miközben növelik a hatékonyságot.

4. A kínált megoldások összemérése és a legerősebb kiválasztása

Az előző fejezetben bemutattam tíz gyártó kínálatát, leginkább a sajátosságokat emeltem ki. Mindegyiknél törekedtem, hogy ismertessek erősségeket és gyengeségeket is. Az SD-WAN a hálózat egy olyan szegmense, ami évről évre nagy ütemben fejlődik, ezért a gyártók szándéka, hogy lépést tartsanak egymással és ne essenek vissza az aktuális piaci helyzetükhöz képest. Sok cég van a piacon, az említett tíz azért került kiválasztásra, mert vagy domináns szereplők, vagy a sajátosságaikkal képesek megfogni a célzott közönségüket.

Az összehasonlításban a szoftver definiált nagy kiterjedésű hálózat elengedhetetlen aspektusaival vizsgálom meg, mely gyártó hogyan teljesít. Egyes kategóriákban szükséges alkategóriát létrehozni, mert egymástól annyira eltérő funkciót látnak el, hogy nem lehet őket azonos osztályzattal pontozni. Ezek a következők:

- Fogyasztási modellek
    - SaaS modell – Ez a modell széles körben elterjedt a felhő szolgáltatások megjelenésétől számítva. A gyártó virtualizált környezetében építi ki főleg a kontroll környezetet és a kész termékhez nyújt hozzáférést.
    - Menedzselt szolgáltatás modell – Ez az üzemeltetés kiszervezését jelenti egy erre szakosodott harmadik félnek. Célja, hogy a környezetet egy képzett csoport támogassa és felszabadítson terhelést a cég saját csapatainak.
    - DIY modell – „Csináld magad” elvről szól, a vevő saját maga építi ki a környezetet és kezeli az infrastruktúrát. Népszerű nagy vállalatoknál, ahol meg van a kellő számú képzett ember.

- WAN technológiák támogatása - Például hibrid környezet támogatottsága különböző privát és publikus vonalak terén, virtuális peremeszközök, kapcsolat összekötés (Link Bonding) a nagyobb sávszélesség érdekében.

- Applikációk hiba elleni védelme és azok megelőzése – A megoldásnak részletes átláthatóságot kell nyújtania az applikációkra és az infrastruktúrára külön bontva. Korszerű probléma felmérő és izoláló technikákat kell támogatnia, hogy a lehető legkevesebb ideig tartson megoldani őket. Lehetővé kell tennie a megfelelő applikáció szegmentálást, hogy redukálja a hibás domének méretét.

- Biztonsági technikák – A hangsúly a tűzfal, VPN, behatolást és adatvesztést megelőző megoldásokon van. Ezek mellett fontos szempontok a malware szűrés, titkosítási metódusok (például 3DES, AES, RSA…) és hogy ezek integrálhatók legyenek a forgalomirányítókba is

- Skálázhatóság és átjárhatóság

    - Hardver és szoftver skálázhatóság – Fontos, hogy a hálózatban hány lokáció, azoknak hány vonaluk lehet. Ide tartozik a kontrollerek skálázhatósága is és hogy mennyi végpontot tudnak kezelni. Ezek mellett a hálózat topológiájából adódóan kérdéses, hogy az eszközök hány virtuális csatornát képesek kiépíteni egyidőben.
    - Gyártó és technológia átjárhatóság – Egy ideális környezetben akár több gyártó megoldása és különböző technológiák találkozhatnak, amiknek működniük kell a hálózaton. ide tartozik még a tradicionális hálózati megoldásokkal való kompatibilitás. Fontos szempont, főleg, amikor a vállalatnak technológia váltás közben az egyik irodája már az új módszerrel működik, de egy másik még a régivel.

- WAN optimalizáció – A megoldásoknak támogatniuk kell jól működő optimalizációt a nagy kiterjedésű hálózatra. Lehetőséget kell biztosítani személyre szabott QoS konfigurációra.

- Hálózat hibaellenállása – Kontrollerek meghibásodása esetén a hálózatnak tovább kell tudnia működni. Fontos az útvonal vizualizáció támogatás, mivel a forgalom keresztül megy fizikai és virtuális hálózaton is. Képesnek kell lenni lekövetni ezeket az útvonalakat, valamint mérni a teljesítményüket. Dinamikus kapcsolat átállást kell biztosítania, mint például az ismertetett útválasztó szabály megfelelő alkalmazása.

- Beavatkozás mentes támogatás – Ide olyan elemek tartoznak, amik segítenek az egyszerű üzemeltetésben. Ilyen a Zero Touch Provisioning, azaz a rendszer fel tud állni a vevő beavatkozása nélkül is. Továbbá automatizáció, analitika, és változtatás kontroll. Utóbbinak a lényege, hogy a lehető legkevesebb ráfordítással lehessen változtatásokat végezni szabályokkal, topológiával, útvonal információkkal.

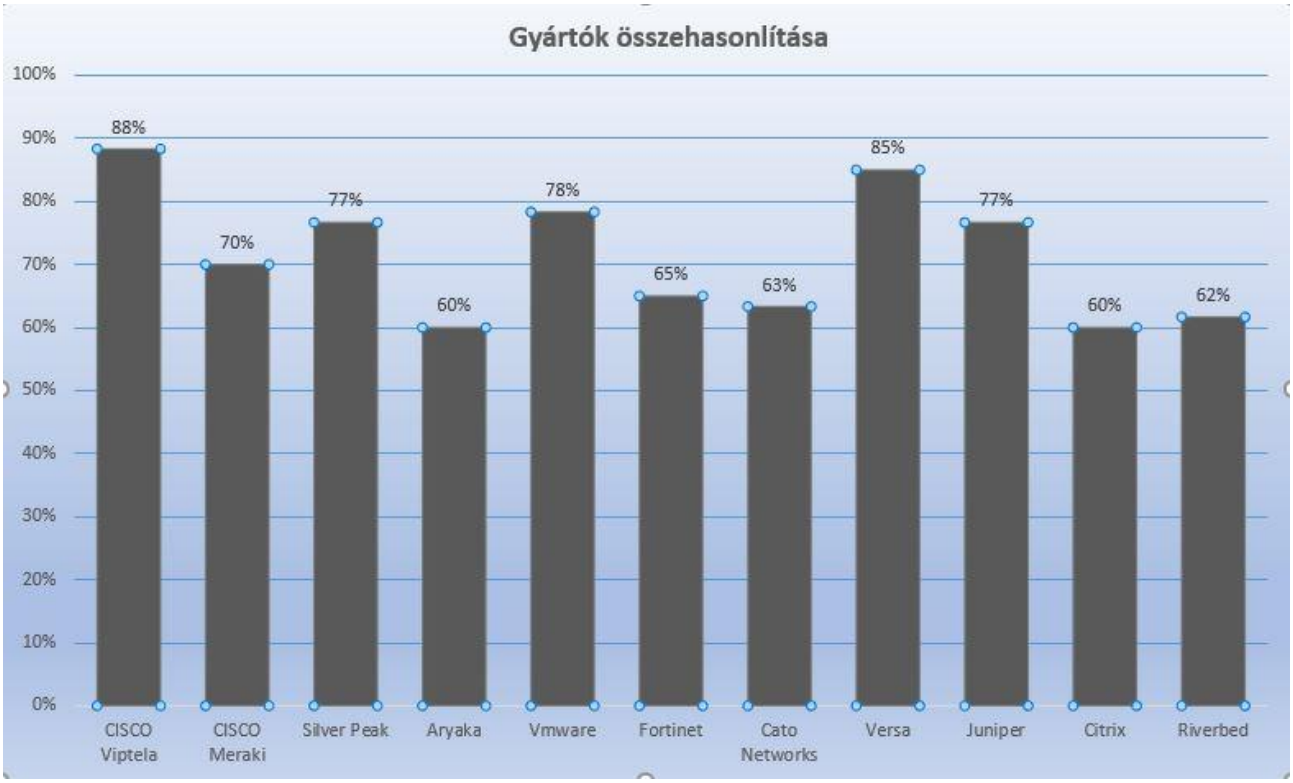
- Felhő alapú szolgáltatások elérése – A megoldás képes legyen a lehető legoptimálisabb útvonalakat kiválasztani a felhasználók számára az applikációk felé.

Ezeket a szempontokat egyenként osztályozom minden gyártóval. Az osztályzatokat 0 és 5 között osztok, ahol a 0 a legkevésbé jó és 5 a kiváló. Ezek után táblázat segítségével szemléltetem, hogy az adott gyártók milyen értékeket ér el a kategóriákba. Ebből készített diagram segítségével százalékos értéket érnek el a kiadható legtöbb pontból. A cél a lehető legjobb lehetőség megtalálása.

Gyártók osztályzása kategóriák alapján:

		CISCO Viptela	CISCO Meraki	Silver Peak	Aryaka	Vmware
Fogyasztási modellek	SaaS modell	5	4	4	2	5
	Menedzselt szolgáltatás modell	4	3	4	4	4
	DIY modell	4	4	4	1	4
WAN technológiák támogatása		5	3	3	4	3
Applikációk hiba elleni védelme és azok megelőzése		4	3	4	3	4
Biztonsági technikák		4	4	3	3	
Skálázhatóság és átjárhatóság	Hardver és szoftver skálázhatóság	5	3	3	2	5
	Gyártó és technológia átjárhatóság	5	4	3	3	5
WAN optimalizáció		4	3	5	3	4
Hálózat hibaellenállása		4	3	4	3	4
Beavatkozás mentes támogatás		4	4	5	4	5
Felhő alapú szolgáltatások elérése		5	4	4	4	4

		Fortinet	Cato Networks	Versa	Juniper	Citrix	Riverbed
Fogyasztási modellek	SaaS modell	2	2	5	4	2	3
	Menedzselt szolgáltatás modell	3	4	5	4	4	4
	DIY modell	4	3	4	4	3	4
WAN technológiák támogatása		3	3	4	4	3	3
Applikációk hiba elleni védelme és azok megelőzése		3	3	4	4	3	3
Biztonsági technikák		5	5	5	3	3	3
Skálázhatóság és átjárhatóság	Hardver és szoftver skálázhatóság	3	3	4	4	2	3
	Gyártó és technológia átjárhatóság	3	3	4	4	3	1
WAN optimalizáció		3	3	3	3	4	4
Hálózat hibaellenállása		4	3	4	4	3	3
Beavatkozás mentes támogatás		2	2	5	4	4	3
Felhő alapú szolgáltatások elérése		4	4	4	4	2	3



A kutatás eredményén látszik, hogy a kisebb gyártók is próbálnak felkapaszkodni és jó eredményeket elérni fejlesztések terén. A nagyobbak konzisztensen jobb minőségű megoldásokkal kínálják terméküket minden téren.

A táblázat mutatja, hogy vannak gyártók, akik nagy figyelmet fordítanak egy-egy fő kategóriára. Célközönségüknek kedvező lehet ár/érték arányban ez a filozófia. Az én értelmezésemben leginkább a nagyobb és komplexebb hálózatok vannak előtérben. Az erre tervezett megoldások inkább kompatibilisek egyszerűbb hálózatokhoz is, mint fordítva.

Két gyártó emelkedik ki technológiailag, a CISCO és a Versa. A mérésem alapján a CISCO három százalékkal magasabb értéket kapott. Mióta a Viptela-t felvásárolta és zászlós hajójává tette az SD-WAN piacon, olyan dinamikus fejlődésen ment keresztül a termék, ami elvárható egy ekkora vállalattól. Az általam meghatározott főbb kategóriák mindegyikében remekül teljesít innovatív megoldásaival.

Ez egy jelenlegi állapot. Folyamatos bejelentéseket adnak ki a gyártók különböző fejlesztésekről, próbálva leküzdeni a gyengeségeiket. Ahogy az informatika technológiái fejlődnek, úgy kell a szoftver definiált nagy kiterjedésű hálózatnak is reagálnia. Ilyen fontos területek például a mesterséges intelligencia vagy az 5G.

Utóbbi elterjedése egy fontos mérföldkő lesz a hálózat világában. jelenlegi tesztek azt mutatják, hogy a gyorsasága és a megbízhatósága vetekszik a fizikai kapcsolatokkal. Ennek eredményeképpen a gyártók már most is dolgoznak azon, hogy integrálható lehessen a szoftver definiált hálózatokba.

Szó szerint idézve: „Iparági konszenzus van arról, hogy ennek a megvalósítása csak az új hálózati technológiák felhasználásával érhető el – különös tekintettel a szoftver definiált hálózatokra (SDN)és felhő (cloud) megoldásokra.” (CINKLER TIBOR, SIMON CSABA, SZABÓ ÖRS, SZÉKELY SÁNDOR, JAKAB CSABA, 2015, p. 42 , https://www.hte.hu/documents/10180/1727937/HT_2016-1_MJIK2015_6_Cinkler_Simon_Szabo_Szekely_Jakab.pdf)

A felmérések és az előrejelzések alapján nagy szerepe lesz a jövőben a szándék alapú hálózatoknak (Intent-Based Networking – IBN). Ennek alapja a mesterséges intelligenciával történő üzemeltetés. Képes lesz tanulni és fejlődni, anomáliákat megoldani. Ez főleg jellemző a kiberbiztonsági fenyegetésekre, ami napjainkban a legnagyobb problémát okozza.

Az egyik, ha nem a legnagyobb kihívást az informatikai szakemberek hiánya okozza. Ez jelentősen lassítja a digitális átalakulást. Egyre jobban előtérbe kerül, hogy a szakembereknek rutin feladatait, mint például eszközök konfigurálása, összetett üzleti problémák technológiával történő támogatása váltsa fel.

Egy másik probléma, hogy a globális nagyvállalatok átállása tradicionális megoldásról szoftver definiáltra nem egy gyors folyamat. A stratégiai és pénzügyi döntéseknek nagy súlya van. Emellett egy nagy hálózatnak is hiába logikus a felépítése, komplexitása lassítja a folyamatokat. Világszerte minden lokáción át kell alakítani az infrastruktúrát, újra tervezni a szolgáltatóktól bérelt vonalak összetételét. Ehhez olyan hálózati csapat kell, akik értenek a szoftver definiált nagy kiterjedésű hálózatok működéséhez és emellett a döntéshozóknak tisztában kell lenniük azzal is, hogy vállalatuknak melyik gyártó terméke felel meg. (CISCO, 2020)

5. Összefoglalás

A szakdolgozatom témája a szoftver definiált nagy kiterjedésű hálózat. Első sorban bemutattam, hogyan működik a technológia és miképpen változott meg a tradicionális megoldásokhoz képest.

Annak szemléltetése érdekében, hogy érthető legyen az újítások fontossága, folyamatosan szemléltettem a tradicionális nagy kiterjedésű hálózat azonos funkciót ellátó részeit. A rendszer strukturálisan változott meg azzal, hogy a vezérlő síkot kiemelték a fizikai eszközökből és egy virtuális központosított irányítást hoztak létre. Idő és erőforrás spórolható meg a hálózat üzemeltetése terén. Az SD-WAN célja, hogy a lehető legautomatikusabban működhessen, egyszerű legyen a skálázhatóság és a fogyasztóknak leegyszerűsítse a technikai kihívásokat.

A vezérlő rendszer elemei automatikusan felismerik egymást és sikeres kapcsolódást követően máris elkezdődhet a hálózat személyre szabása. A hálózati menedzsment felületen tud a felhasználó mindent beállítani. Ezek az információk átkerülnek a kontrollerekhez, amik az automatikus irányítást feladatát végzik. Ők továbbítják az adatokat a perem eszközöknek, amik a vállalat lokációin vannak elhelyezve. A központi menedzselésnek köszönhetően egyszerű manipulálni a topológiát szabályok létrehozásával.

Ezek a szabályok váltják fel a klasszikus értelemben vett hálózati konfigurációt. A tradicionális megoldásban parancssoros interfészen keresztül kell sokszor egyenként elvégezni forgalomirányítókon a változtatásokat. Személyes tapasztalatom szerint es alkalmakként hibalehetőségekhez vezet, mint például elírások, amiket nem vesz észre az ember. Az SD-WAN ellenben grafikus felhasználói felületet biztosít, így nem kell bonyolult parancsokat használni. Egyszerűségével és átláthatóságával megkönnyíti a szakemberek munkáját. A szabályoknak külön kategóriája van, más-más céllal. A tervezéskor fontos odafigyelni és jól definiálni az egyes elemeket és a belőlük alkotott listákat. A szabályok hivatkozás alapon működnek, szóval, ha a példa kedvéért a lokációk

egy bizonyos csoportjára szeretne a felhasználó szabályt alkotni, előre el kell készíteni a lokációk listáját, a szabályban érvényesülő protokollokat és hasonló elemeket.

A szabályok fő kategóriái a kontroll szabályok, ami vezérlő síkon értelmezendő, adat, útválasztó, biztonsági és hálózat optimalizáló szabályok. Ezeken belül széles skálája van, hogy mit lehet beállítani, a hálózat kezelőin múlik és azon, ahogyan megtervezték az infrastruktúrát.

A szélessávú Internet fejlődésével adott a lehetőség, hogy a drága bérelt vonalak jobban háttérbe szoruljanak annak érdekében, hogy költséghatékony legyen a hálózat. Fontos viszont, hogy az Internet még mindig a legtöbb esetben „best effort" alapon működik, azaz nincs garancia arra, hogy 100%-os megbízhatóságot nyújt az adattovábbításhoz.

Erre olyan megoldásokat alkalmaz a szoftver definiált nagy kiterjedésű hálózat, amivel pontos és valós idejű méréseket képes végezni a rendszer. Döntéseket hoz, hogy adott forgalom éppen milyen vonalon menjen a lehető legjobb felhasználói élmény elérésének érdekében. Képes értelmezni és kezelni a hagyományos protokollokat, mint például BGP vagy OSPF. Emellett saját fejlesztésű protokollokat hoznak létre a gyártók, ami a megfelelő módok tudja kezelni a szoftver definiált hálózat kommunikációját. Támogatnia kell az aktuális újításokat.

Az SD-WAN korszerű biztonságot és szegmentációt nyújt a domének között. Kiemelt figyelem van a kiberbiztonságon, mint például a malware szűrés. Ezt a legtöbb gyártó dinamikusan oldja meg, a rendszer minták alapján tanulja meg a fenyegetések tulajdonságait és szűri ki. A megfelelő szegmentációs lehetőségekkel izolálni lehet a hálózat részeit elérés szempontból. Szabályozni lehet, hogy bizonyos szegmensek kiket érhetnek el és kik által érhetők el.

A mai trendek alapján nagy hangsúly van a felhő alapú szolgáltatásokon. A vállalatok nagy része kiszervez olyan szolgáltatásokat, mint például levelezés, pénzügyi rendszerek vagy a profiljukhoz szükséges alkalmazások. Legjobb példák a SaaS alapú termékek, mint az Office 365 levelező applikáció. A tradicionális megoldásban ezek elérése a gyakorlatban legtöbbször úgy néz ki, hogy a felhasználó kezdeményezi a kapcsolatot az irodából, a forgalom először bemegy a vállalat adatközpontjába és onnan jut el a felhő szolgáltatóhoz. Ez fölösleges utak megtételéhez vezet. Az SD-WAN egyik

fő tulajdonsága, hogy felépítésének alapjaitól szempont a felhő alapú szolgáltatásokhoz a minőségi kapcsolat biztosítása.

Külön lehet kezelni a menedzsment felületeken az applikációkat és a hozzájuk tartozó kapcsolatokat. Erre fejlesztett tesztek és funkciók segítik elő az optimális kapcsolatok kialakítását a felhasználó és a szolgáltatás között.

A technológia ismertetése után a szakdolgozat második részében a kutatásom keretein belül ismertettem tíz gyártót a piacról. Kiválasztásuk aszerint történt, hogy piacvezető technológiával rendelkeznek vagy olyan célzott területen nyújtanak kimagasló teljesítményt, hogy a célközönségük számára optimális választási lehetőség legyen. A fő különbségek a kínálatok között az, hogy a gyártók az SD-WAN technológiába milyen további megoldásokat tudnak integrálni. Ezek lehetnek jól ismert korábbi vagy újonnan fejlesztett termékeik. A rohamos fejlődés miatt változó, kinek van a legjobb megoldása bizonyos problémákra. Kiemeltem fő szempontokat, amik elengedhetetlenek a szoftver definiált nagy kiterjedésű hálózat alapvető működéséhez és pontoztam a gyártok azokban nyújtott teljesítményét. A végeredmény egy felállított rangsor, ami alapján a CISCO Viptela megoldását találtam a legjobbnak. Tapasztalatom szerint is egy remek opció.

Személyes véleményem a szoftver definiált nagy kiterjedésű hálózatról, hogy korszerűsége elengedhetetlen a vállalatok fejlődésében. Olyan korlátokat küzd le és ezáltal olyan lehetőségeket nyújt, amit a tradicionális hálózatok már nem tudnak teljesíteni, vagy csak nagyon a határokat feszegetve. Ennek hátránya, hogy nagymértékben nő a komplexitása és a kezelhetősége. Kaput nyit a mesterséges intelligenciák alkalmazására a hálózat üzemeltetéséhez. Megalapozza a hálózat jövőbeli fejlődését. A legnagyobb hátrányának azt tartom, hogy a szakma így is szakember hiányban küzd. Az új technológia az emberek bizonyos szintű átképzését igényli. Az ilyen hatások azt hozzák magukkal, hogy a vállalatok digitális átalakulása lassabban történik, mint ahogy azt az SD-WAN lehetővé teszi.

Mindent összevetve a szoftver definiált hálózat egy hiánypótló megoldás a felhő szolgáltatások elterjedésével születő igényekre. Ahogy a szakma, én is kíváncsian várom, hogy az új évtized milyen fejlesztéseket hoz még magával és hogy milyen ütemben folytatódik a technológia elterjedése a tradicionális hálózatok mellett.

6. Irodalomjegyzék

CISCO digitális anyagok az SD-WAN bemutatásáról

https://digital-learning.cisco.com/#/course/60680 - Letöltve: 2020. március 13.

https://digital-learning.cisco.com/#/course/60687 - Letöltve: 2020. március 13.

https://digital-learning.cisco.com/#/course/60681 - Letöltve: 2020. március 17.

https://digital-learning.cisco.com/#/course/60686 - Letöltve: 2020. március 19.

https://digital-learning.cisco.com/#/course/60692 – Letöltve: 2020. március 22.

2015-ös Magyar Jövő Internet Konferencia címen kiadott tudományos cikk

CINKLER TIBOR, SIMON CSABA, SZABÓ ÖRS, SZÉKELY SÁNDOR, JAKAB CSABA, 2015

https://www.hte.hu/documents/10180/1727937/HT_2016-1_MJIK2015_6_Cinkler_Simon_Szabo_Szekely_Jakab.pdf - Letöltve: 2020. április 2.

Szolgáltatás láncolás fogalma

https://whatis.techtarget.com/definition/service-chaining – Letöltve: 2020. április 14.

SD-WAN gyártók bemutatása

https://www.netify.co.uk/learning/comparison-top-14-sd-wan-providers-vendors – Letöltve: 2020. április 23.

SD-WAN gyártók bemutatása

https://www.netify.co.uk/learning/top-best-sd-wan-providers-vendors – Letöltve: 2020. április 23.

A Cisco előrejelzése: technológiai trendek a 2020-as évekre

https://www.cisco.com/c/hu_hu/about/press/archives-2020/20200115.html – Letöltve: 2020 április 30.

SD-WAN gyártók piaci helyzete és előrejelzések

https://www.appsruntheworld.com/top-10-sd-wan-software-vendors-and-market-forecast-2018-2023/ - Letöltve 2020. április 30.

Cikkek SD-WAN gyártók fejlesztéseiről

https://virtualizationreview.com/articles/2019/04/22/versa-titan.aspx – Letöltve: 2020. május 1.

https://virtualizationreview.com/articles/2019/12/05/juniper-sdlan.aspx – Letöltve: 2020. május 1.

https://virtualizationreview.com/articles/2019/03/11/citrix-security.aspx – Letöltve: 2020. május 2.

https://virtualizationreview.com/articles/2019/05/21/riverbed-sdwan-saas.aspx – Letöltve: 2020. május 2.

https://virtualizationreview.com/articles/2020/01/06/fortinet-challenge.aspx – Letöltve: 2020. május 3.

https://virtualizationreview.com/articles/2020/02/12/fortinet-moves.aspx – Letöltve: 2020. május 3.

https://www.sdxcentral.com/networking/sd-wan/definitions/aryaka-managed-sd-wan/ - Letöltve: 2020. május 3.