1. RENDSZERERŐSÍTÉS

Az információ biztonsági stratégia kialakítása során a hangsúly mindig a megelőzésen kell, hogy legyen, a támadások azonosítása előtt. A rendszer kialakítása és folyamatos felügyelete során szükség van a használt rendszerelemek és konfigurációk olyan kialakítására és beállítására, ahol a sérülékenységek rosszindulatú vagy hibákból adódó kihasználhatóságának az esélyét a minimumra tudjuk csökkenteni.

1.1. A rendszeridő megfelelő beállítása

A biztonsági incidensek felderítések során alapvető követelmény, hogy a naplózási fájlok a megfelelő időbélyeggel legyenek ellátva. A gyakorlatban a rendszeridő nem minden esetben kerül beállításra az eszközökön és előfordulhat, hogy nincs a megfelelő időzónában, illetve nincs szinkronban az időátállítással.
A felderítés során fontos tudni, hogy a támadó milyen sorrendben lépett be bizonyos eszközökbe. A legtöbb országban a támadó nem ítélhető el, ha a naplóbejegyzések időbélyegei nem meggyőzőek vagy megkérdőjelezhetőek. Minden hálózati eszköznek illetve naplózási fájlt tároló szervernek szükséges, hogy legyen olyan elérhető és megbízható időforrása, ami biztosítja a pontos időt és NTP[1]-t használ.

1.2. Szükségtelen szolgáltatások és protokollok leállítása

A Cisco IOS rendszerrel összehasonlítva az NX operációs rendszer alapértelmezésben nem futtat olyan TCP illetve UDP alapú szolgáltatásokat, melyek távolról elérhetők. Ezáltal nincs olyan szolgáltatás, amit esetlegesen le kellene állítani. A Cisco NX operációs rendszer moduláris felépítésű. A funkciói olyan protokollok, melyek a saját védett memória tartományukban futnak. Hogy milyen funkció indítható el azt alapvetően meghatározza, hogy milyen licensz került telepítésre. Az elérhető funkciókat parancssoron keresztül lehet aktiválni illetve deaktiválni (például OSPF, TACACS+). Alapértelmezésben nincs egyetlen funkció sem elindítva.

1.2.1. CDP letiltása minden megbízhatatlan interfészen

[1] Network Time Protokol

A Cisco Discovery Protocol a Cisco saját fejlesztésű protokollja, ami azt a célt szolgálja, hogy ezek az eszközök könnyen azonosíthassák egymást a helyi hálózaton, ezáltal megkönnyítve a például a hibaelhárítást. De ez ugyanúgy használható az esetlegeses támadók által is a hálózat könnyebb feltérképezésére. Alapértelmezésben a CDP be van kapcsolva a NX-OS rendszerekben. Le kell tiltani minden olyan esetben azokon a portokon, amik valamelyik DMZ VLAN-jához kapcsolódnak, illetve ha az dedikálva van valamelyik végfelhasználóhoz. Mivel ez csak a Cisco gyártótól származó eszközökön használható megfelelő módon, ezért heterogén hálózati infrastruktúra esetén ezt a funkciót le kell tiltani.

1.2.2. HTTP szerver letiltása

Bizonyos NX operációs rendszereket futtató eszközök esetében egy web interfészen keresztül engedélyezve van a web alapú adminisztráció. Ez megköveteli, hogy egy kisebb http szerver fusson az eszközön. Amennyiben ez a szerver fut, az eszköz elérhető titkosítatlan HTTP protokollon keresztül. Azon kívül, hogy úgymond grafikus felületet biztosít, nem kínál plusz szolgáltatást a parancssorral szemben, ezért ezt a funkciót le kell tiltani.

1.2.3. DNS domain lookup

Alapértelmezésben engedélyezve van a funkció, mely a hosztok neveit egy DNS szerver segítségével IP címmé tudja fordítani. Ez azt eredményezi, hogy az eszköz broadcast DNS lekérdezéseket végez, amit egy támadó kihasználva erre hamis információkkal tud válaszolni. Tehát ezt a funkciót mindenképp helyesen fel kell konfigurálni, vagy ellenkező esetben le kell tiltani.

1.2.4. Proxy ARP

"A forgalomirányítók a broadcast (szórt) csomagokat nem továbbítják. A forgalomirányítók Proxy ARP szolgáltatást biztosítanak, ha ez a szolgáltatás engedélyezve van rajtuk. A Proxy ARP az ARP protokoll egy változata. Ennél a változatnál a forgalomirányító a megfelelő MAC-címet tartalmazó ARP-választ küld a kérést kibocsátó állomásnak azon az interfészen, amelyen a kérés beérkezett. Azokra a kérésekre, amelyekben az IP-cím nem esik a helyi alhálózat címtartományába, a forgalomirányítók saját MAC-címükkel válaszolnak. Az

alapértelmezett átjáró címe az állomások egyik hálózati beállítása, amely a forgalomirányító interfészének IP-címét adja meg. A forrásállomás a célállomás IP-címének és saját IP-címének összehasonlításával megállapítja, hogy a két IP-cím ugyanabban a szegmensben van-e. Ha a célállomás nem azonos szegmensbe esik, akkor a forrásállomás a célállomás IP-címével és a forgalomirányító MAC-címével küldi el az adatokat. A forgalomirányító MAC-címét az állomás az ARP-táblából, a forgalomirányító IP-címe alapján keresi ki. "[13]

A gyakorlatban bizonyos virtuális környezetben és tűzfalak számára szükség lehet erre a funkcióra. NX-OSben alapértelmezésben be van kapcsolva ez a funkció és központilag ezt nem is lehet lekapcsolni csak az interfészeken. Amennyiben nincs rá szükség, de mégis bekapcsolva marad, úgy egy támadó felhasználhatja úgynevezett man in the middle támadásra vagy adott forgalmak elkapására.

1.2.5. IP source routing

Habár alapértelmezésben ez a funkció be van kapcsolva és egyfajta öröklött funkció, csak nagyon ritka esetekben van rá szükség és ezért központilag le kell tiltani.

1.2.6. ICMP és ICMP továbbítás

Különösen az ezredforduló idején az ICMP[2] üzenetek felhasználása nagyon népszerű volt különböző felderítő típusú támadások esetében. Az ICMP egy interneten használt protokoll, melynek segítségével értesülhetünk a hibákról illetve azok típusáról, valamint hálózati diagnosztizálásban lehet a segítségünkre. Összességében megállapíthatjuk, hogy az ICMP teljes letiltása nem teszi döntően eszközünket biztonságosabbá, viszont sokkal nehézkesebbé válhat adott esetben a felügyelet valamint a hibaelhárítás. Az ICMP használatának konfigurálása során arra kell figyelni, hogy az eszközünk ne váljon úgymond erősítőjévé az ICMP csomagok továbbításával egy smurf támadásnak, ne lehessen túlterhelni ICMP csomagokkal (sem egy esetleges támadás vagy hálózati hiba esetén), illetve hogy az a loopback és menedzsment interfészeken le legyen tiltva.

1.2.7. SNMP protokoll letiltása

[2] Internet Control Message Protocol

Az SNMP a Simple Network Management Protocol, azaz az egyszerű hálózat menedzsment protokoll rövidítése. Az SNMP protokoll egy egyszerű "kérdezz-felelek" protokollnak tekinthető, ahol az NMS[3]-en futó alkalmazások folyamatosan vagy egy előre meghatározott időközönként lekérdezik a felügyeleti eszközökhöz rendelhető változókat, amelyek valamilyen választ fognak adni további feldolgozás céljából. Lényeges, hogy egy elosztott felügyeletű protokollról van szó, amely a hálózatra kötött eszközök vezérlését, adatainak lekérdezését szolgálja. Mostanra három verzió létezik. Az SNMP v1 és SNMP v2 biztonsági szempontból ugyanazt a metódust használja és ugyan mindhárom verzió elérhető NX OS-ben, használni csak az SNMPv3 javasolt. SNMPv3-ban már nem nyílt szövegben zajlik az azonosítás, hanem titkosítva ezáltal növelve a hálózatbiztonságot. [14]
Az SNMP NX operációs rendszerben az SNMPv3 alapértelmezésben engedélyezve van. Amennyiben az SNMP nincs jelentős mértékben használatban, ebben az esetben javasolt letiltani az eszközben.

1.2.8. IPv6

Az IPv6 a legutolsó verziója az internet protokollnak. Amíg az utóbbi években még nem terjedt el széles körben, napjainkban már láthatjuk használatban. A földrajzi elhelyezkedéstől függően az IANA[4] 2011 januárban az ARIN[5] pedig 2011 áprilisban beszüntette az IPv4 publikus címek regisztrálását.
Elméleti szinten napjainkban már minden hálózati eszköz és szerver/kliens operációs rendszer IPv6 képes. Kivételt képezhetnek bizonyos SSL és IPSEC VPN implementációk, személyes tűzfalak és biztonsági megoldások, valamint néhány szerver szoftver termékek. Ha helyesen van konfigurálva az IPv6 nagyon sok előnyt hozhat, és pozitív változásokat jelenthet.
NX operációs rendszerben szinte minden szolgáltatás használható IPv4 és IPv6 címzéssel. Alapértelmezésben az IPv6 le van tiltva addig, amíg egy Layer 3-as interfészhez IPv6-os cím kerül hozzárendelésre. OSPF alkalmazása esetén arra kell figyelni, hogy csak az OSPF 3-as verziója támogatja az IPv6-ot. Ebben az esetben ezt az OSPF verziót kell aktiválni. A BGP és statikus route kezelni tudja az IPv6-ot. Jelenleg a legéletképesebb konfiguráció, ha mind az

[3] Network Management System
[4] Internet Assigned Numbers Authority
[5] American Registry for Internet Numbers

IPv4 és IPv6 elérhető adott eszközön. Az IPv4 és IPv6 hálózatok közötti hibák és átfedések kiküszöbölésére VACL[6]-t - VLAN hozzáférési listákat lehet létrehozni.

1.3. Vezérlési sík biztonságosabbá tétele

NX operációs rendszerben megkülönböztetünk három síkot, ezek a management plane (üzemetetési sík), control plane (vezérlési sík) és a data plane (adat sík. Mindhárom síkot megfelelően kell konfigurálni, erősíteni és ezzel biztonságosabbá tenni.
A vezérlési sík (control plane) irányítja a transzportréteg hálózati elemeit és végzi el a végpontok között szükséges kapcsolatok felépítését. Az ezen a szinten kell az eszköznek "megértenie" a hálózati topológiát, illetve döntéseket kell hoznia az adatfolyam- és hálózatvezérlés kapcsán. Legfontosabb feladata, hogy a mindenkori körülmények figyelembevételével biztosítsa az akadályoktól és fennakadásoktól mentes hálózati adatforgalmat. Ennek érdekében folyamatosan tanulnia, és minden lényeges paraméterét feltérképeznie kell a hálózatnak, illetve az ahhoz csatlakoztatott eszközöknek. Ezzel biztosítható például, hogy egy hiba következtében kieső, akár több hálózati eszköz se okozzon leállást a teljes hálózati adatforgalomban. A hálózati eszköz szempontjából vezérlési síkon haladó csomagoknak mindig van egy fogadó IP címe és a hálózati forgalmat bonyolító processzort használják.

1.4. Biztonsági funkciók engedélyezése

1.4.1. IP Source Guard (IP forrás cím védelem)

Egy hálózat üzemét hamis DHCP szerver beüzemelése alaposan megzavarhatja rossz IP címek kiosztásával, és ily módon a hálózat használata lehetetlenné válik (DoS támadás). Kényes állapot az is, amikor egy hamis DHCP szerverről hamis gateway/router cím kerül kiosztásra a kliensek számára, így térítve el az alapértelmezett gateway/router felé tartó forgalmat. A hamis gateway az ily módon hozzá irányított forgalmat észrevétlenül (a hálózat működik) tudja lehallgatni.
Az NX OS eszköz fenntart egy ARP táblát, amelyben ethernet címek tárolódnak a hozzájuk tartozó IP címekkel. Ez alapján történik az eszközök által az elküldendő adatkeretek címzése.

[6] VLAN Access Control List (

Ha egy állomás egy adott IP címmel rendelkező állomással akar kommunikálni és nem tudja az ethernet címet, egy ARP kérést küld a hálózatra, amelyet az adott IP címmel rendelkező állomás megválaszol majd. Az ARP kérés ethernet broadcast formájában minden eszközhöz eljut, de megválaszolni alapesetben csak a cél-IP címmel rendelkező eszköz fogja. Az ARP mechanizmus kompromittálásával lehetséges bármely két kommunikáló fél közé beékelődni és észrevétlenül lehallgatni a teljes kommunikációt. Továbbá az ún. gratuitous ARP válaszok elfogadásának engedélyezése nem a cél-IP címmel rendelkező eszköztől érkezik, hanem egy harmadik kommunikáló féltől, mintegy segítségként.[15]
Az NX OS rendelkezik egy minden DHCP történést rögzítő táblázattal (DHCP binding table), amelyet az ethernet kapcsolók építenek fel a DHCP forgalom monitorozásával. Az eszköz megvizsgál és összevet mindent ARP kérést és választ a DHCP binding táblázatban található információval, és amennyiben egy ARP válasz nem az ARP-tulajdonostól (azaz az IP cím jogos tulajdonosától) származik, az eldobásra kerül. A jogosult ARP-tulajdonos egy olyan port, amelyen lévő eszköz a DHCP-táblában megtalálható a megfelelő ethernet és IP címmel rendelkezik.
IP forrás cím védelme (IP source guard) egy védelmi szolgáltatás, mely az előbb említett DHCP binding táblázatot használja a címek ellenőrzésére. A táblázatban megtalálható, hogy a kapcsoló mely portján milyen IP című eszköz csatlakozik. Ha más forrás IP címmel rendelkező adatcsomag lépne be egy adott kapcsoló porton, mint ahogy az a táblázatban szerepel, akkor azt az eszköz eldobja.

1.4.2. uRPF

Az Unicast Reverse Path Forwarding arra szolgál, hogy limitálhassuk hálózatunkon a gyanús hálózati forgalmat oly módon, hogy ellenőrzésre kerül a forrás cím elérhetősége. Ezzel kizárható, hogy hamis címről tudjanak az eszközünkre forgalmat generálni. Amennyiben a forrás IP cím nem létezik, a csomag eldobásra kerül. Három különböző típust kerülhet beállításra. Ezek a szigorú és megengedő üzemmódok illetve a VRF[7]. Szigorú módban az az elvárás, hogy a csomagnak azon az interfészen kell érkeznie, amin az eszköz a válaszcsomagot egyébként visszaküldené. Ennek az alkalmazása során fenn áll a veszély, hogy aszimmetrikus útvonal választási módok esetén legális csomagok eldobásra kerülhetnek. Megengedő üzemmódban a forráscímnek csak az irányítási táblában kell megjelennie. [16]

[7] Virtual routing and forwarding

Az uRPF szolgáltatást használata javasolt minden Layer 3-as "megbízhatatlan" eszközhöz vagy WAN-hoz kapcsolt interfészen. Habár önmagában ez a szolgáltatás nem jelent teljes biztonságot, nagyban hozzájárul az esetleges támadások szűréséhez.

1.5. Layer 2 switch portok biztonságosabbá tétele

Cisco adatátviteli kapcsolókon a Layer 2-es interfészeket portoknak nevezzük. Azokon a kapcsolókon, ahol a port security nincs alkalmazva egy adott szabad porton, egy támadónak lehetősége nyílik saját eszköz csatlakoztatására információszerzés vagy támadás céljából. Habár az utóbbi öt nyolc évben a kapcsolók már nem érzékenyek számottevően az ARP spoofingra illetve CAM[8] tábla elárasztásra támadóknak még mindig lehetősége van rosszindulatú eszközök csatlakoztatására és azon keresztül támadások végrehajtására.

1.5.1. Alapértelmezett port viselkedés

NX operációs rendszerekben minden port Layer 3-as port. Ez azt jelenti, hogy úgy viselkednek, mintha egy forgalomirányító eszköznek a portjai lennének. A gyakorlatban ezeknek a portoknak többségére inkább Layer 2-es szinten van szükség, ezért NX OS-ben lehetőség van az erre történő, azaz az adatkapcsolati rétegben történő használathoz való átállítására. Javasolt ezt a módosítást elvégezni minden portra, ha ennek nem az ellenkezője a kívánatos.

1.5.2. Nem használt portok letiltása

A nem használatos portok letiltása a leggyorsabb és leghatékonyabb módja annak, hogy megakadályozzuk illetéktelen eszközök csatlakoztatását hálózatunkhoz. Ugyanakkor mivel azok a saját kliensek helyére is csatlakoztathatók ezért ennek a jelentősége amennyiben a fizikai védelem nem megoldott alacsony. Mindenesetre a legjobb gyakorlat ezeknek a portoknak a letiltása és a használatban lévő portok időközönkénti ellenőrzése.

1.5.3. Errordisable recovery

[8] Content addressable memory

NX operációs rendszer képes a valamilyen hiba folytán letiltott portok visszaállítására. Abban az esetben, ha szeretnénk az egyszeri hibákból vagy egyéb ideiglenes problémákból adódó port letiltásokat hamar megoldani, konfigurálhatunk errordisable visszaállítási funkciót. Ez abban az esetben javasolt, ha a port letiltása BPDU[9] guard, failed-port-state vagy link-flap hibából adódik. Alapértelmezésben 300 másodperc a visszaállítás időintervalluma.

1.5.4. Port security

A port security megakadályozza a nem engedélyezett MAC[10] címekkel rendelkező eszközök csatlakozását. A port security segítségével megelőzhető, hogy egy nem engedélyezett eszköz csatlakozni tudjon egy adott használatban nem lévő, de nyitott porton keresztül. Az is elérhető, hogy egy engedélyezett eszköz (például nyomtató) lekapcsolásával és annak helyére csatlakozással hozzáférjenek a hálózathoz. A támadónak lehetősége van eszközének MAC címének az engedélyezettre történő cseréjére, de a port security jelezni fog.
Három konfiguráció lehetséges, melyek a statikus, dinamikus és sticky metódus. Statikusan megadhatók az engedélyezett MAC címek egy adott kapcsoló porton, vagy – beállítható, hogy a kapcsoló dinamikusan tanuljon meg előre meghatározott számú MAC címet egy adott kapcsoló portra vonatkozóan. A statikus konfigurálás nem egy skálázódó megoldás, így üzemi környezetben a dinamikus megközelítés javasolt. A portonként engedélyezett MAC címek számának 1 -re állításával a hálózat kontroll nélküli növekedése megelőzhető, és az illetéktelen hozzáférések kiszűrhetők. Amint a MAC címek egy védett porthoz való hozzárendelése megtörtént, onnantól kezdve az a port nem továbbít olyan beérkező kereteket, amelyek forrás MAC címe a definiált MAC címek csoportjában nem található meg.

53. táblázat: A három különböző metódus áttekintése

Metódus	Újraindítás után megmarad	Tanulási folyamat
Statikus	Igen (a runnig-config része)	Manuálisan konfigurált
Dinamikus	Nem	A biztonságos MAC címek maximális számáig
Sticky	Igen (NVRAM-ban tárolt)	A biztonságos MAC címek maximális számáig

[9] Bridge Protocol Data Units
[10] Media Access Control

Mindhárom metódus esetén az aktív portokra meg tudjuk határozni, hogy mi történjen adott támadás vélt vagy valós esetén. Ez úgynevezett büntetési (violation) mód, ami lehet csomageldobás (protect), csomageldobás és erről üzenetküldés (restrict) valamint port letiltás (shutdown) is. A port letiltás a legbiztonságosabb megoldás. Az első két esetben további vizsgálatokra van szükség és az több processzoridőt igénylő tevékenységet eredményez.

54. táblázat: A három különböző büntetési mechanizmus összehasonlítása

Büntetési mód	Továbbítja a forgalmat	Küld rendszerüzenetet	Mutat hibaüzenetet	Lekapcsolja a portot
Protect	Nem	nem	nem	Nem
Restrict	Nem	igen	nem	Nem
Shutdown	Nem	igen	nem	Igen

NX operációs rendszereken lehetőség van a Port Security Aging használatára is, aminek segítségével beállítható egy adott időintervallum a statikusan vagy dinamikusan konfigurált biztonságos MAC címek kiöregedésére az adott porton. Két típusa támogatott az öregedésnek:

- absolute: a biztonságos címek a porton a beállított öregedési idő lejártával törlődnek;
- inactivity: a biztonságos címek a porton akkor törlődnek, hogyha nem tapasztalható aktivitás az előre megadott ideig.[17]

1.6. VLAN és trönkök

A VLAN[11] azaz virtuális helyi hálózat tagjai broadcast módon, azaz úgy kommunikálnak, mintha ugyanabba a szórási tartományba tartoznának, fizikai elhelyezkedésüktől függetlenül. Egy VLAN ugyanazokkal a jellemzőkkel bír, mint egy fizikai helyi hálózat (LAN), de lehetővé teszi az eszközök együtt kezelését még akkor is, ha nem ugyanarra a hálózati kapcsolóra csatlakoznak.

NX operációs rendszer alapvetően a porthoz rendelt VLAN tagságot használja, ami azt jelenti, hogy egy adott portot hozzá lehet rendelni a megfelelő VLAN-hoz. Például az 1-5ig portok hozzá vannak rendelve a VLAN 100-hoz és a portok 6-8ig pedig a VLAN200-hoz. A kapcsoló

[11] Virtual Local Area Network

érzékeli a VLAN tagságot azzal, hogy megvizsgálja adott csomag melyik portról érkezett. A másik fontos tényező a VLAN implementációja során, hogy NX operációs rendszer csak a 802.1Q beágyazást használja a csomagok VLAN tagságának címkézésére ellentétben az IOS rendszerekkel, ahol a Cisco ISL (Inter-switch) és IEEE[12] 802.1q VLAN trönkölési metódusok is használatban vannak.

A VLAN szeparáció hatékony határokat szabhat az adatforgalmaknak. Kialakításának számtalan oka lehet, mind a teljesítményfokozás és mind a QoS[13] terén. „*A VLAN jelölő információkat másként VLAN azonosítónak (VID[14]) is hívják. A portok egy kapcsolón egy VLAN tagjaiként vannak beállítva, amelyet a VID jelöl ki az adott port számára. A port alapértelmezett VID azonosítóját nevezik Port VID-nek (PVID) is.*" [18]

1.6.1. Rendszer VLAN-ok

Alapértelmezésben minden port a VLAN 1-es VLAN azonosítóhoz (VID) van rendelve. Ez szintén az alapértelmezett érték a trönk interfészekhez. Ez azt okozhatja, hogy bizonyos portok ebben a VLAN-ban maradva megoszthatják vagy kiterjeszthetik a hálózatunkat anélkül, hogy mi ezt szeretnénk. Ez nagyban megkönnyíti az esetleges támadók dolgát. Amennyiben adott rendszeren úgy döntünk, hogy VLAN-ok használatára szükség van, ebben az esetben a VLAN 1-et nem szabad használni, és minden nem allokált portot egy másik VLAN-ba át kell helyezni.

1.6.2. Privát VLAN-ok

A privát VLAN-okat a gyakorlatban körülbelül egy évtizede ismerhetjük, amikor azzal a céllal kezdték el használni, hogy megerősítsék a külső védelmet és később a demilitarizált zónák biztonsági helyzetét. Ebben az időben a VID-ek száma még 1024-ben volt korlátozva és a tűzfalak még szűkös erőforrásokkal, valamint mindössze három vagy négy fizikai porttal rendelkeztek. Ahogy folyamatosan a korlátozások eltűntek a PVLAN-ok nagyon népszerűek lettek azáltal, hogy lehetővé tették például ugyanahhoz a Gatewayhez, de egymástól elszeparálható ADSL felhasználók kapcsolódását, vagy adott esetben lehetővé tették WLAN kapcsolóktól a megbízhatatlan kliensek elszeparálását. Meg kell jegyezni, hogy rosszul vagy

[12] Institute of Electrical and Electronics Engineers
[13] Quality of Service
[14] VLAN ID

hiányosan konfigurált PVLAN konfiguráció inkább nagyon veszélyes, mint hasznos. A privát VLAN-ok úgy korlátozzák egy szegmensen belül a kiszolgálók közötti forgalmat, hogy azt a 2. rétegben választják szét, a broadcast szegmenseket nem broadcast, többszörös hozzáférésűhöz hasonlatos szegmensekké alakítják.
Napjainkban minden tűzfal támogatja a fizikai interfészen történő VLAN címkézést, ahol a VID-ek száma maximum 4048 lehet (amennyiben NX-OS-t használunk, mint hálózati core.) Minden olyan szerver, amit szeparálni szeretnénk a hálózaton, kaphat egy dedikált VLAN-t és kaphat egy saját DMZ-t. A PVLAN napjainkban elavult és ajánlott valódi VLAN-ok és valódi DMZ-k használata ezért az NX rendszer implementálásakor nem ajánlatos használni.

1.6.3. VLAN hozzáférési listák

VLAN ACL[15]-ek megakadályozzák a jogosulatlan hálózati hidak kialakítását a VLAN-okon belül. Ehhez úgynevezett VLAN térképet használnak. Ennek a térképnek a segítségével szűrni lehet a VLAN-ok közötti kommunikációt. Ugyanaz a VLAN térkép szűri a kimenő, bejövő és átmenő forgalmat adott VLAN-hoz. Javasolt ennek a funkciónak a használata, hogy meg tudjunk akadályozni a nem kívánt VLAN-okon belüli forgalmat. Ez lehet például nem kívánatos IPv6 forgalom.[19]

1.7. VDC használata

VDC[16] használatával egyesíthetjük és újragondolhatjuk meglévő, de korábban egymástól elkülönített hálózatainkat. Ha korábban két vagy több szeparált hálózatunk volt, akár különböző szinten is volt minősítve, a VDC technológia segítségével mindezt egyetlen eszközön helyezhetjük el úgy, hogy a fizikai eszközön több virtuális eszközt hozunk létre saját irányítási és továbbítási feladatok elvégzésére. Ez a hálózati forgalom és a menedzsment valós szegregációját jelenti, mert mindez független hardver és szoftver részegységekkel megoldott. Minden VDC rendelkezik saját konfigurációs adatbázissal tehát a kapcsolás, irányítás és a biztonság ezáltal független minden VDC-ben.
A rendszer előnyei, hogy csökkenti a költségeket, mivel kevesebb eszközre van szükség, amivel azoknak a tápellátása és hűtési igénye is csökken. A meglévő portok különböző rendszerekhez történő allokálását dinamikusan tudjuk végezni, azaz ha az egyik rendszeren vannak felesleges

[15] Access Control List
[16] Virtual Device Context

portok, az a másikhoz hozzárendelhető. Hagyományos megoldásnál port hiány esetén új eszközt kell vásárolni. Mivel különböző hálózatokat vonunk össze kevesebb eszközön ezért a szükséges eszközök száma drasztikusan csökkenthető. Nincs szükség annyi forgalomirányítóra és kapcsoló eszközre. A másik nagy előnye, hogy az üzemeltetés nagymértékben egyszerűsödik azáltal, hogy például kevesebb eszközön kell a biztonsági frissítéseket, a szolgáltatásokat és biztonsági szabályokat frissíteni. Adott esetben csak egy fizikai eszközt kell menedzselnünk. Az új konfigurációk tesztelése, kapcsolódási paraméterek beállítása és elkülönített tesztkörnyezet kialakítása könnyedén megvalósítható egy szeparált VDC-ben anélkül, hogy rendszereinkre az bármilyen negatív hatással lenne. A kompartmentalizáció[17] magasabb biztonságot jelent, mint a virtuális forgalomirányítás és továbbítás (VRF - Virtual Routing and Forwarding) és VLAN-ok használata.

Tételezzük fel, hogy szeretnénk létrehozni két különálló hálózatot. Az egyiket rendszerünk nyílt, míg a másik bizalmas információkat tartalmaz. A fizikai eszközünkön létre kell hoznunk egy-egy VDC-t, amik saját irányítási síkkal fognak rendelkezni, azaz saját dedikált adminisztrátor tudja a szükséges L2 és L3 protokollokat és szolgáltatásokat (STP, BGP, OSPF, stb.) használni csakúgy, mintha egy különálló fizikai eszközön tennék azt. Minden VDC adminisztrátornak csak a saját VDC-jéhez és irányítási síkjához van hozzáférése. Cisco NX 70xx eszközökben maximum négy VDC-t lehet létrehozni.

1.8. Feladatátvétel és redundancia

1.8.1. Spanning Tree Protokol (STP)

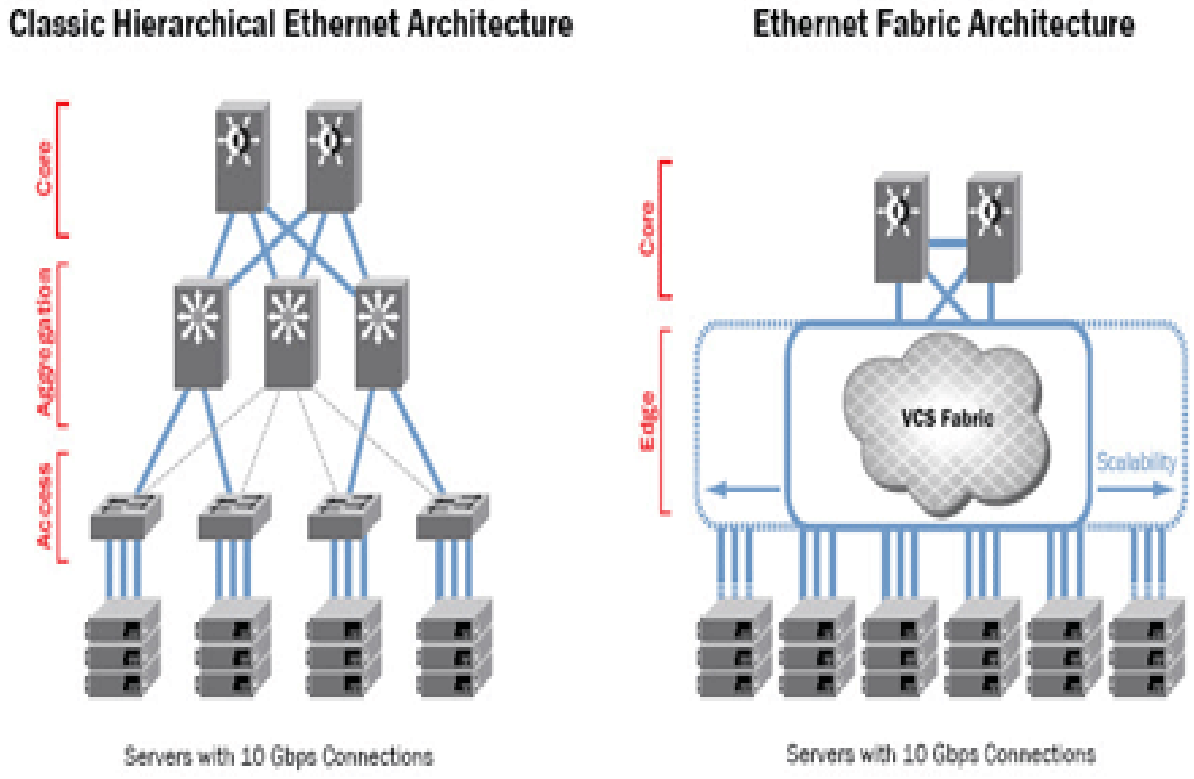
A hibatűrés redundanciával érhető el. A nagy megbízhatóságú hálózatokban redundáns útvonalakat és készülékeket kell elhelyeznünk. Egy redundáns topológiában egyetlen elem meghibásodása nem okoz teljes körű leállást. Amint egy eszköz vagy vonal meghibásodik egy másik eszköz vagy útvonal veszi át a helyét. Az irányítási hurkok azért jönnek létre, mert a redundáns kapcsolók nem foglalkoznak egymás jelenlétével. Ezért fejlesztették ki a feszítőfa protokollt, hogy megoldja ezt a problémát és ki tudjuk használni a redundáns kapcsolatok előnyeit. A STP célja tehát a hurokmentes topológia kialakítása, másfelől pedig szakadás esetén a redundáns tartalék kapcsolat mielőbbi felélesztése.[20] Az STP egy minimális konfigurálást igénylő, lényegében önállóan működő protokoll. Azok a kapcsolók, melyeken engedélyezett az

[17] rekeszesítés, kazettásítás

STP az első bekapcsoláskor ellenőrzik a kapcsolt hálózatok esetleges hurkait. Hurok észlelésekor letiltják az érintett portok valamelyikét, míg a többi porton aktív marad a kerettovábbítás. Az első széles körben elterjedt implementációt a DEC készítette. A protokollt később az IEEE szabványosította.
Az aktuális IEEE szabványok:

- Spanning Tree Algorithm and Protocol: 802.1D-1998, 802.1t-2001
- Rapid Spanning Tree Algorithm and Protocol: 802.1w-2001 (802.1D-2004)
- Multiple Spanning Tree Protocol: 802.1s-2002, 802.1Q-2003 [21]

Éveken keresztül mindenki az STP-ben látta a megoldást a Layer-2es hurkok elkerülésére. Azonban megállapítható, hogy ezres switch port számnál már adott esetben az STP kalkuláció percekig is eltarthat, ami negatívan befolyásolja más szolgáltatások működését, és például alkalmazása csökkenti az elérhető VID-ek számát is. A 2010-es év környékén a változott a tendencia és a gyártók az úgynevezett Ethernet Fabric irányába fordultak. Az Ethernet Fabric olyan innovatív szövet, ami lehetővé teszi a csomagok továbbításánál azt, hogy egy csomag belépjen egy kapcsolóra, feldolgozásra kerüljön és így elhagyja az eszközt (routolva, NAT-olva, szűrve, stb.) anélkül, hogy inter-chassis/inter-switch kommunikációra lenne szükség.



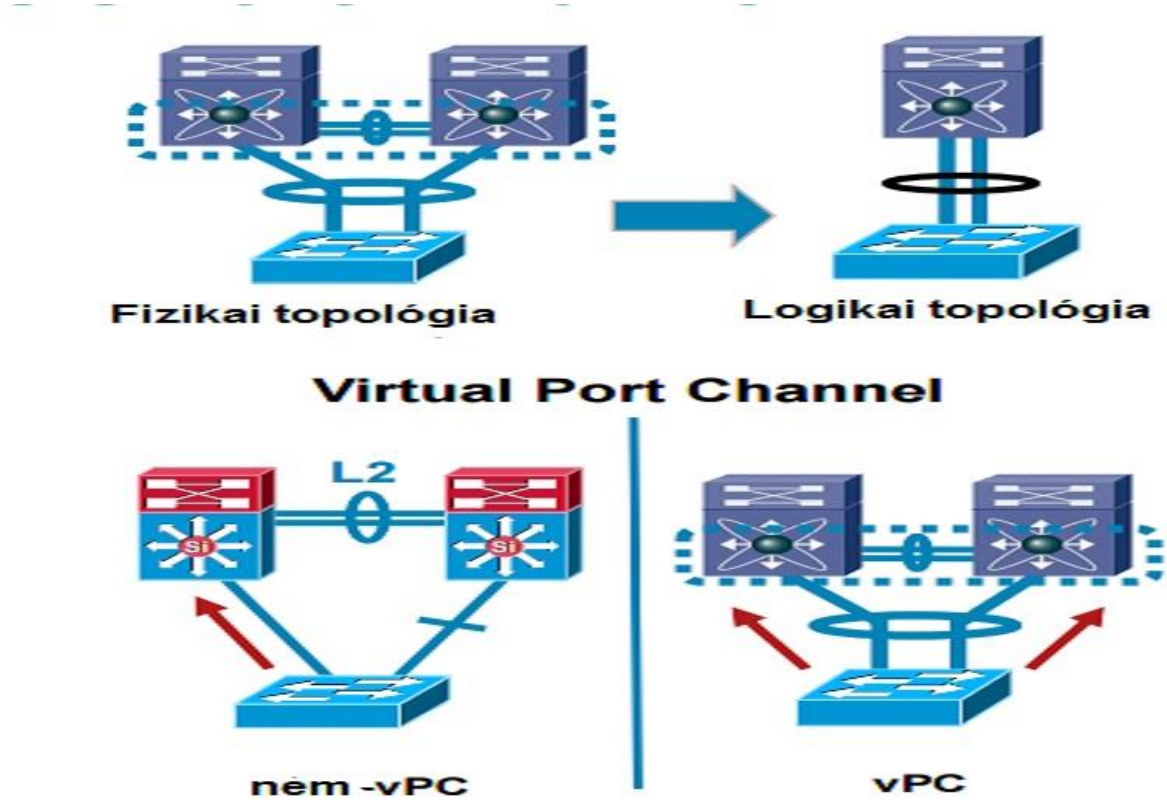
4. ábra: Hagyományos és Ethernet Fabric megoldás összehasonlítása

NX operációs rendszerben nem találhatók az IOS rendszerekben rendelkezésre álló STP parancsok. Ez a rendszer az IEEE 802.1D és IEEE 802.1W szabványokat használja. Egyedül a PVST+[18]-t használja. PVST+ segítségével egy kapcsolón különböző STP példányokat hozhatunk létre minden egyes VLAN-nak. A kapcsolók azonosítójához hozzáadódik egy VLAN ID, amely lehetővé teszi, hogy minden VLAN-nak saját root bridge-je, root port-jai és egyéb STP eszközei legyenek. A fejlesztéssel optimalizálhatjuk az adatforgalmat és terhelés eloszlást valósíthatunk meg a kapcsolók STP működése között.

1.8.2. Virtual Port Channel

A PVST+ (és ezáltal az STP) buktatóit elkerülendő az NX operációs rendszer két lehetőséget kínál ezek alternatívájaként. Az egyik a már említett Ethernet Fibre (ez külön licensz igényes) és a másik megoldás a vPC[19]. A vPC egy Port-channeling koncepció, ami a link aggregációt valósít meg. Ez redundáns L2 topológia alapú link aggregáció, ami szükségtelenné teszi az STP-t az access-distribúciós rétegek között. Mindezzel sávszélesség növelést biztosít, mivel az összes link egyidejűleg aktív.

[18] Per VLAN Spanning Tree +
[19] Virtual Port Channel



5. ábra: vPC fizikai és logikai topológiák összehasonlítása

1.9. Menedzsment sík védelme

1.9.1. Alapértelmezett VDC adminisztrátori felhasználó és jelszó

NX operációs rendszerekben léteznek különböző felhasználók megfelelő szerepkörökkel. Minden VDC (még a root VDC is) rendelkezik egy beépített admin felhasználóval, akinek a legmagasabb hálózati rendszergazdai jogosultsága van. A root VDC admin felhasználóját nem lehet eltávolítani. Egyéb VDC-k admin felhasználóit lehet törölni, de újra létrehozásra fognak kerülni a felhasználó következő bejelentkezésekor. Az eszköz tartalmaz egy gyárilag elhelyezett jelszó komplexitást meghatározó szabályt, ami megköveteli a következő kritériumoknak történő megfelelést:

- legalább nyolc karakter hosszúnak kell lennie;
- nem tartalmazhat túl sok egymás után következő karaktert (például abcd);
- nem tartalmazhat szótári szavakat;

- nem tartalmazhat ismétlődő karaktereket (például aaa);
- nem tartalmazhat neveket (például Peter);
- tartalmaznia kell nagy, illetve kisbetűket;
- tartalmaznia kell számokat.

1.9.2. AAA keretrendszer javasolt használata

Az AAA keretrendszer nélkülözhetetlen az NX operációs rendszert futtató eszközök biztonságosabbá tételéhez. Ez az egyetlen és legfontosabb része az eszközhöz és a VDC-khez történő biztonságos hozzáféréshez. Minden AAA konfiguráció egyedi a VDC-k esetében, ami azt jelenti, hogy adott konfiguráció csak az adott VDC-re érvényes. NX operációs rendszerekben az AAA használata egyszerű és főleg a hitelesítésre fókuszál, habár biztosít további elszámolhatósági szolgáltatást is. Az NX operációs rendszer támogatja a TACACS+ és RADIUS hálózat biztonsági szolgáltatásokat, ahol inkább a TACACS+ a preferált megoldás. Az AAA konfigurációja a rendszerben egyszerű és csak két lépésből áll. Az első lépés során megadhatjuk a távoli szerver paramétereit vagy a helyi hitelesítési információkat attól függően, hogy melyik megoldást választjuk. A második lépésben pedig beállítjuk az AAA hitelesítés metódusát.

1.9.3. Helyi és távoli szerveren történő hitelesítés összehasonlítása

Az AAA lehetővé teszi az adminisztrátorok számára, hogy a biztonsági szolgáltatásokat akár helyi vagy egy távoli biztonsági eszközön tárolt információkra alapozzák. Az első megoldás akkor megoldható, ha hálózati eszközök száma nem túl magas. Ennek a megoldásnak az előnye, hogy nincs egy központi elem, aminek a kompromittálódása esetén annak minden hálózati elemre történő kihatása lenne. Valamint ha minden eszközön különböző jelszó van, akkor egy jelszónak a megszerzése még nem jelent veszély más eszközökre. Ugyanakkor a helyi szolgáltatás nem skálázható. Amikor több hálózati eszközünk van, szükségszerű egy központi biztonsági eszköz alkalmazása. Az NX operációs rendszer három biztonsági protokollal képes kommunikálni. Ezek a TACACS+, a RADIUS és az LDAP (Active Directory). Az AAA hálózati protokollok mindegyike magában foglalja a jelszavak bizalmasságának védelmét a hálózati eszköz és a biztonsági szerver között. Ugyanakkor nem védi a jelszót a hálózati eszköz és a távoli adminisztrációs munkaállomás között. Annak érdekében, hogy a jelszó nyílt szövegként kerüljön továbbításra SSH használatára van szükség.

1.9.3.1. Helyi hitelesítés

A helyi hitelesítés helyi adatbázist használ, melyben tárolásra kerül a felhasználónév és a hozzá tartozó jelszó. Ez abban az esetben használható, ha a hálózat relatíve kicsi és nem tartalmaz túl sok hálózati elemet. Minden NX operációs rendszerben tárolt jelszó Type-5 típusú titkosításra kerül, mielőtt az eszköz eltárolja a konfigurációs fájlban.

1.9.3.2. TACACS+ hitelesítés

A TACACS+ a Cisco saját hozzáférési protokollja. Előnye, hogy TCP-t használ, letitkosítva a teljes csomagot az Access Control Server (hozzáférési szerver, ami a TACACS+ szolgáltatást biztosítja) és az NX operációs rendszer között. Hátránya, hogy csak Cisco termékek esetében használható, szóval, ha más gyártók termékeit is használjuk a hálózaton, akkor a RADIUS-t kell használnunk. Egy előre megosztott kulcs biztosítja a titkosított kommunikációt a kapcsoló és a biztonsági szerver között. A kulcs biztonságossága és minősége nagyon fontos tényező ezért nagyon hosszú kulcsot érdemes választani, amit adott esetben a felhasználónak már ne legyen lehetősége csak úgymond begépelni.

1.9.3.3. Radius hitelesítés

A Radius hozzáférési szerver protokoll a Livingston Enterprises által lett kifejlesztve és az RFC 2845ben lett dokumentálva. A Radius sokkal több gyártói platformmal együttműködik a TACACS+-szal összehasonlítva azonban sok hátránnyal rendelkezik:

- a Radius UDP-t használ, míg TACACS+ TCP-t;
- a Radius a jelszót csak a hozzáférési kérés csomagban titkosítja le, míg a TACACS+ a teljes felhasználói adatot;
- A Radius kombinálja a hitelesítési és engedélyezési folyamatokat, míg a TACACS+ külön kezeli ezeket a funkciókat;
- a TACACS+ rendelkezik beépített multiprotokol támogatással.

1.9.4. Felhasználói szerepkörök és szerepalapú hozzáférés vezérlés (RBAC)

Az RBAC[20] szerepalapú hozzáférési jogosultság-kezelés, mint az elnevezésből következik, a hozzáférés ellenőrzésére egy adott szerepkörhöz kapcsolt szabályrendszert használ. A szerepalapú hozzáférés-jogosultsági modellben ahelyett, hogy minden felhasználóhoz specifikus, az adott objektumhoz elérést biztosító vagy tiltó jogosultságokat kapcsolnánk, szerepeket határozunk meg. Minden felhasználóhoz szerepek különböző csoportja rendelhető. A szerepek meghatározzák, leírják, hogy adott szerepkörben milyen objektumon milyen műveletek végezhetők. Azaz az objektumok eléréséhez szükséges jogosultságok nem a felhasználóhoz kapcsoltak, hanem a szerepekhez. Egy-egy felhasználó több szerepet is elláthat. A felhasználó számára az objektumokhoz kapcsolt engedélyek az általa végzendő konkrét feladatokhoz és nem az egyes objektumok biztonsági besorolásához kapcsolódnak.[22]

1.9.5. Felhasználó szerepkörök

NX operációs rendszerekben a felhasználói szerepkörök hasonló funkciókkal bírnak, mint az IOS rendszerekben található hozzáférési szintek. A felhasználó szerepkör olyan szabályokhoz kötött, mely meghatározza, hogy adott felhasználó számára milyen műveletek végrehajtása engedélyezett. Vannak úgynevezett beépített felhasználói szerepkörök, amiknek törlése nem lehetséges.
Alapvető szerepkörök:

- network admin; teljes olvasási és írási joggal a teljes NX operációs rendszerben;
- network operator; teljes olvasási joggal a teljes NX operációs rendszerben;
- VDC admin; olvasási és írási joggal a hozzá tartozó VDC-hez;
- VDC operátor; olvasási joggal a hozzá tartozó VDC-hez.

Alapértelmezésben Nexus eszközbe történő belépés esetén, amennyiben AAA hitelesítés van konfigurálva, a felhasználó az alapértelmezett felhasználói szerepkörhöz fog hozzájutni, ha az másképp nem lett kiválasztva a hitelesítés folyamat során. Amennyiben a rendszer VDC-be történik a belépés, ekkor a network operátor szerepkör lesz elérhető. Ha VDC-be történik a belépés, akkor az adott VDC operátor szerepkör lesz elérhető. Amennyiben az AAA csak hitelesítésre volt konfigurálva, akkor a Nexus eszköz egy TACACS vagy Radius szervertől várja a szerepkör meghatározását, amit a rendelkezésére bocsájtott felhasználói azonosítókból

[20] Role-Based Access Control

határoz meg. Ennek hiányában a korábban említett alapértelmezett felhasználói szerepkör kerül kiadásra. Ha az AAA-ból a hitelesítés és az engedélyezés is megvalósításra kerül, akkor az felülírja, és nem teszi szükségessé az alapértelmezett és egyéni felhasználói szerepkör használatát. RBAC az a képesség a Nexus eszközökben, ami lehetővé teszi egyedi szerepkörök létrehozását és azokhoz jogosultságok hozzárendelését.

2. NX-OS GYAKORLATI ALKALMAZÁSA

Egy képzeletbeli egyetem informatikai rendszerének példáján keresztül bemutatom a meglévő rendszerek és az implementálásra kerülő NX operációs rendszert futtató Nexus eszközök használatát, annak biztonsági aspektusain keresztül.

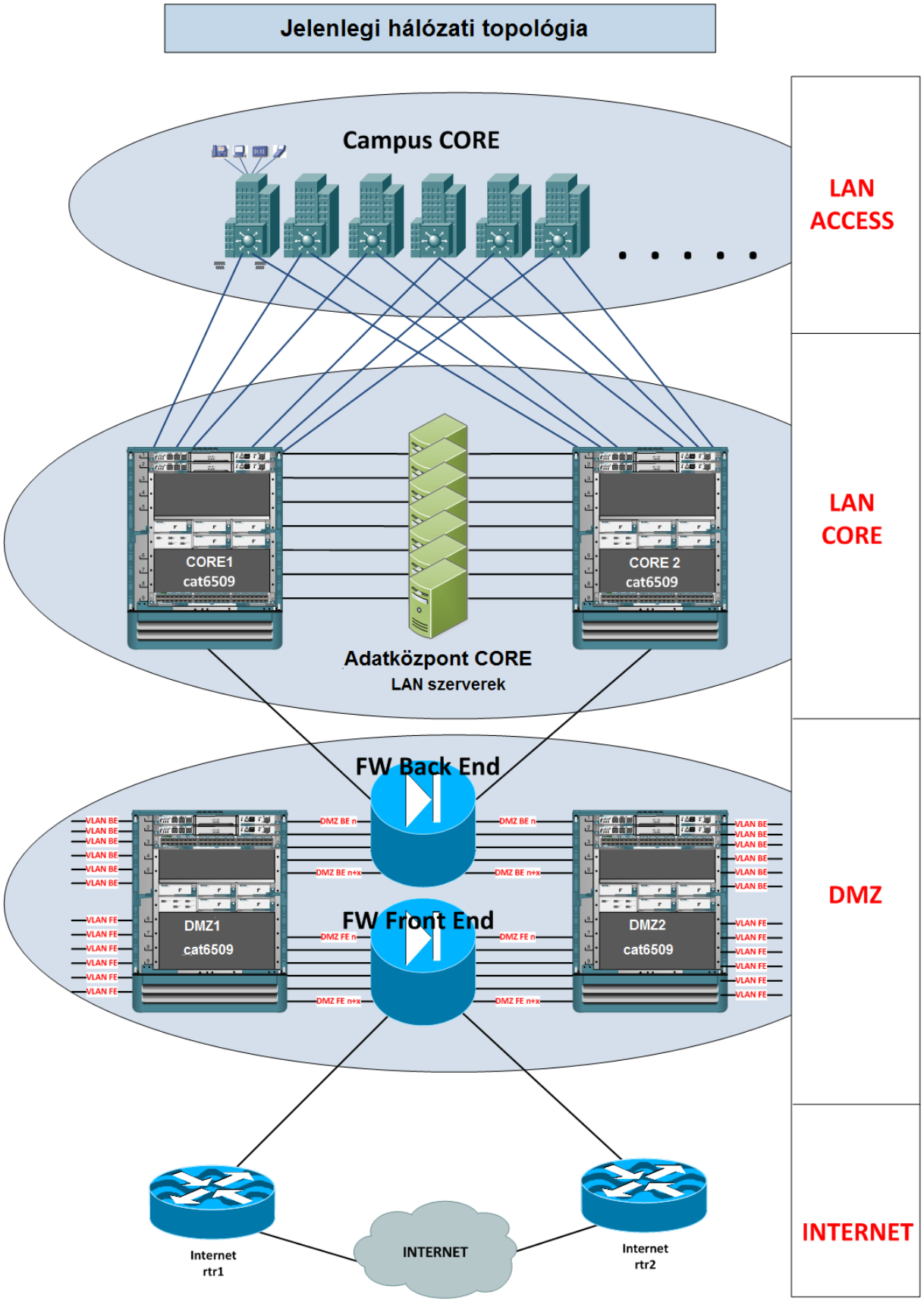
2.1. Jelenlegi rendszer

A jelenlegi rendszerben két fő belső hálózatot különböztetünk meg, melyen az egyik hálózat úgynevezett publikus vagy nyílt hálózat. Ide kapcsolódhatnak diákok illetve az egyetem látogatói és azon keresztül elérhetik a világhálót anélkül, hogy azon különösebb korlátozások lennének. A forgalom monitorozására kerül és a nem megfelelő használat esetén lehetőség van az adott felhasználó rendszerből történő kizárására. A másik hálózat az egyetem dolgozói számára elérhető privát és minősített hálózat, ahol sokkal magasabb biztonsági követelményeknek megfelelően elérhető például levelezési, adattárolási és sok egyéb szolgáltatás.

A jelenlegi hálózat IPv4 és IPSEC/VPN alapú. Az egyetemi LAN úgy épül fel, hogy annak alapját két Core catalyst alkotja (CORE1 és CORE2) és épületenként további catalyst-ok kapcsolódnak hozzá. A SAN egy külön switch-en kapcsolódik Fibre Channelen keresztül a menedzsment VLAN-hoz.

A hálózati szegregáció különálló Front-end és Back-end demilitarizált zónákon alapul, és a kialakított VLAN-ok száma meghaladja a 30-at. A Front-end DMZ kapcsolva van az Internethez és a Back-end DMZ[21]-hez. Mindkét DMZ rendundáns kialakítású, azaz két külön eszközön került kialakításra (DMZ1 és DMZ2). A Front-end DMZ határolja a publikus, míg a Back-end DMZ a privát hálózatot.

[21] demilitarized zone



6. ábra: Jelenlegi hálózati topológia

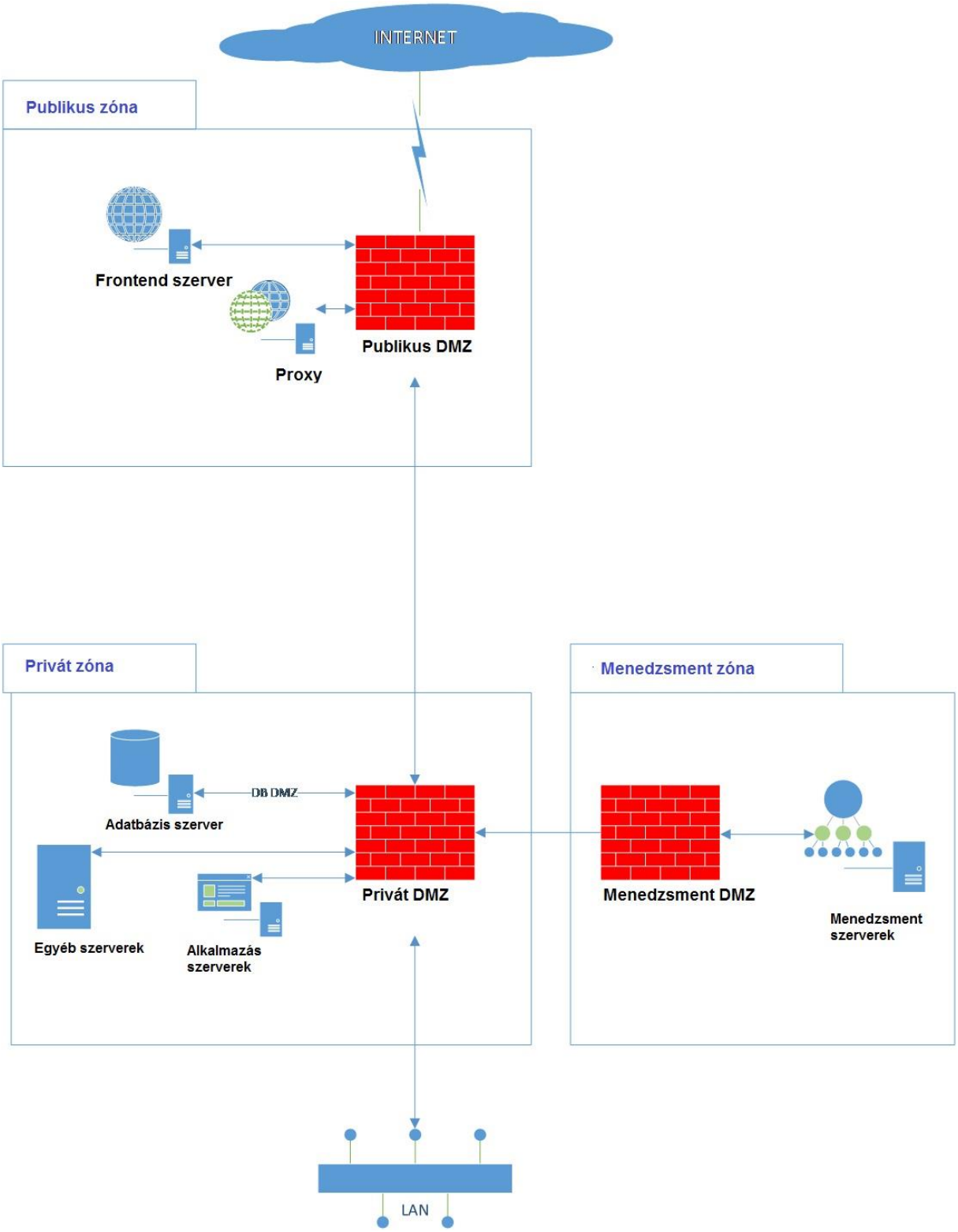
2.2. A hálózat biztonsági architektúra építő kövei

Egy új hálózati infrastruktúra létrehozásakor szükségszerű egy új hálózat biztonsági architektúra létrehozása is, mivel ez megkönnyíti a biztonsági ellenintézkedések kiválasztását és azok indokolatlan átfedések nélküli következetes implementálását. Továbbá megkönnyíti a megfelelőségi vizsgálatokat és auditokat, mivel azt célozza, hogy a kapcsolat a fenyegetések, kockázatok és ellenintézkedések között átláthatóbb legyen. A hálózat biztonsági architektúra kidolgozása összetett feladat, mivel kialakítása üzleti folyamatokat szolgál, melyek követelményei széles spektrumon mozognak. Mindez sokszor bizonyos alkalmazások és hálózati protokollok módosításával jár egy olyan környezetben, ahol az eszközök beszerzése több gyártótól történik és meg kell találni az egyensúlyt a biztonság, a használhatóság és az ár között. A biztonsági architektúrától azt várjuk, hogy:

- védelmezze az infokommunikációs rendszerünket úgy, mint ahogy a biztonsági házirendek és eljárások védik a szervezetet;
- legyen biztonságos (ahogy teljes biztonság nem érhető el, ez abban az értelemben, ahogyan a különböző szabályok, eljárások és szabványok megkívánják);
- legyen arányos (egyensúly kell teremtenie a védelembe fektetett erőforrások és a fenyegetés által okozott kár között, felkészülve a legrosszabb esetre anélkül, hogy túlzásba esnénk.

A Szerző véleménye, hogy amíg az ISO 27001 jó útmutatást kínál a biztonsági ellenintézkedések azonosítására és kezelésére, hiányzik viszont belőle, hogy hogyan lehetne ezeket a gyakorlatban integrálni. További útmutatást találhatunk a NIST publikációkban, úgymint a NIST SP 800-37ben (Guide for Applying the Risk Management Framework to Federal Information Systems), amely bemutatja a kockázatelemzés alapelveit és a felelősségi körök allokálását.

2.3. Védelmi vonalak kiépítése



7. ábra: Védelmi vonalak

A fenti ábrán jól látható a három zóna, melyek elkülönülnek egymástól. Ezek a publikus, privát és a rendszerfelügyeleti zónák kerülnek kialakításra. A zónák további alzónákra oszlanak (DMZ). Ez a struktúra biztosítja számunkra a szervezet hálózat biztonsága szempontjából, hogy

a kritikus érzékenységű szerverek, mint például egy adatbázis, SAP vagy fájlszerver szeparálva legyen legalább két szintű védelmi szintekkel. A zónák további DMZ-kre bonthatók, igény szerint.

A publikus zóna tartalmazza a rendszer azon elemeit, melyeknek közvetlen elérésük van az Internethez. Itt található a proxy kiszolgáló, itt történik a VPN kapcsolatok hitelesítése valamint itt biztosított a megjelenítési réteg a belső alkalmazások részére.

A privát zóna tartalmaz minden egyéb szervert, ami a szervezet mindennapi tevékenységéhez és a felhasználók mindennapi munkájához szükséges. A fenti ábra is mutatja, hogy a DMZ szeparáció alkalmazás szinten történik. Az alkalmazások csoportosítása lehetővé teszi számunkra, hogy a tűzfalon alapértelmezett beállításokat használjunk. Például egy adatbázis VLAN-ra, amiben SQL és Oracle szerverek találhatóak, vonatkozik egy szabályt, ami engedélyezi a forgalmat a 1433 (SQL) és 1521 (Oracle) portokon mindenkinek adott VLAN-ban. Ez segíti további adatbázis szerverek integrációját, amik elérhetőek lesznek ezen alapértelmezett beállításokkal, és a tűzfal nem igényel ilyen irányú további konfigurációt. Ez nem csak felgyorsítja a szerver üzembe helyezést, de csökkenti az egyedi tűzfalszabályok létrehozásával való munkát és csökkenti az esélyét a konfigurációs hibák kialakításának.

A rendszerfelügyeleti zóna tartalmazza az összes felügyeleti kiszolgálót, készülékeket és alkalmazásokat, minden log szervert és egyéb felügyeleti eszközt. Annak ellenére a rendszer belsejében található, hogy kiszolgál eszközöket a publikus zónából is. Ennek a zónának külön tűzfala van, ami ezt a zónát védi. Ezen a menedzsment tűzfalon a szabályokat felhasználók számára kell kialakítani és nem akár IP címek, vagy hálózatok számára.

2.4. NX operációs rendszert futtató Nexus eszközök használata

A Nexus eszközök legjelentősebb újdonsága a VDC (Virtual Device Context) implementálása, mely lehetőséget biztosít a megvásárolt licenszek számától függően virtuális Nexus platformok létrehozására. Minden VDC úgy értelmezhető, mintha egy különálló eszközünk lenne ahol semmilyen illetéktelen adatmozgás nem érhető el két virtuális eszköz között.

Az adminisztratív VDC szerepe, hogy arról minden egyéb VDC elérhető legyen konfigurációs célból anélkül, hogy képes lenne kimondottan adatok továbbítására.

A tárolási VDC úgy kerülhet konfigurálásra, hogy elválasszák egymástól a LAN és SAN forgalmakat.

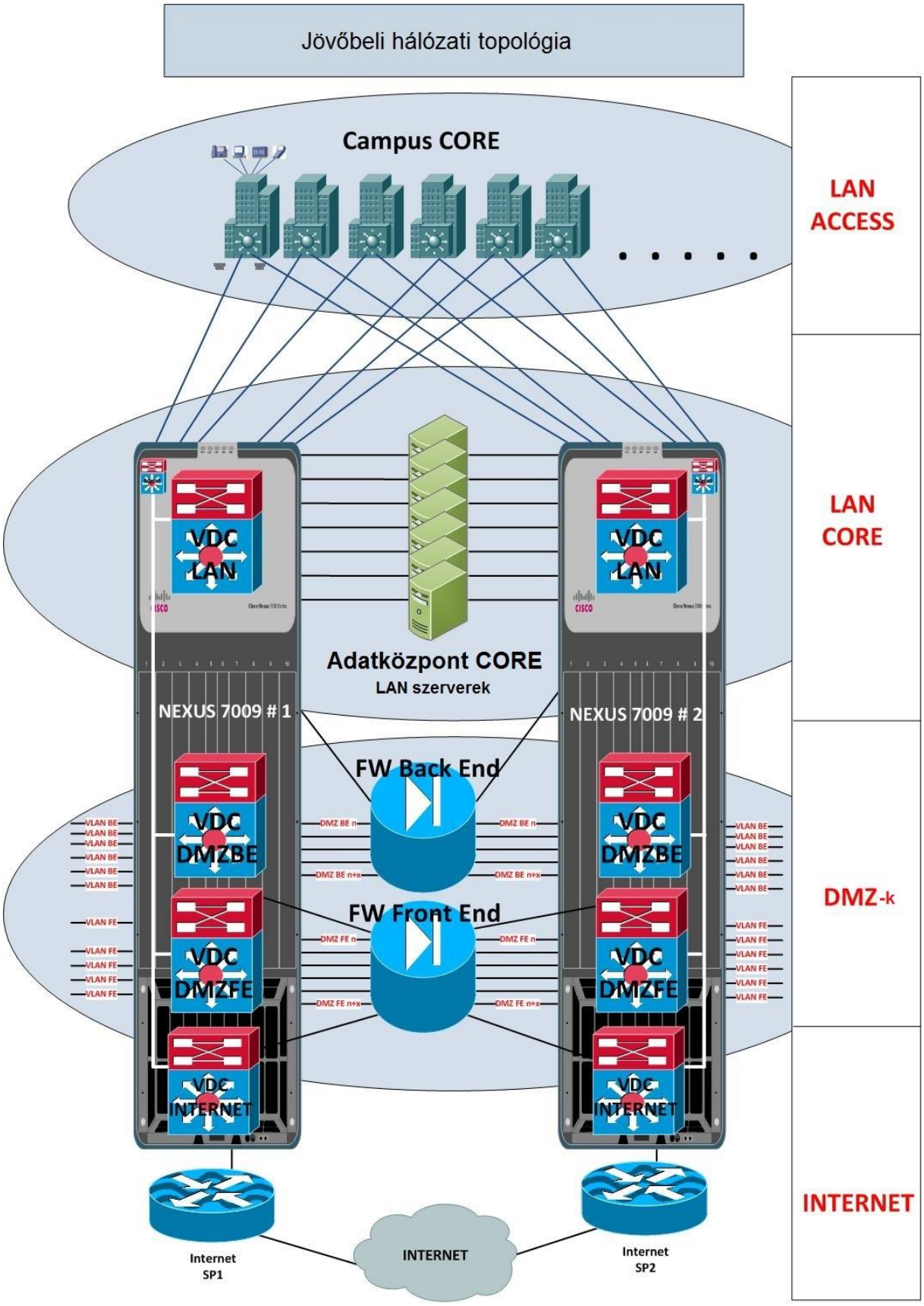
A VDC-k implementálásával úgy növelhetjük a biztonságot, hogy közben nagyban csökkenthetők a költségek is. A jelenlegi konfiguráción látható, hogy a Front-en és Back end DMZ-k ugyanazon az eszközön találhatók. A szeparáció VLAN-ok segítségével történik. Míg ennek segítségével elérünk bizonyos biztonságot, a VLAN-ok átjárhatóságának problémája nyomán sokkal inkább javasolt volna a Back-end és front-end DMZ-k külön eszközön történő elhelyezése. Ez, mint tudjuk, megduplázná a költségeket. Egy Nexus eszközön a VDC funkció bekacsolásával létrehozhatunk virtuális eszközöket, melyek független eszközök, saját konfigurációval, forgalomirányítási táblával és egyedien engedélyezett funkciókkal. És ahogy korábban említve volt a koncepció úgy lett kialakítva, hogy a virtuális eszközök között nem lehetséges az adatátvitel a fizikai eszközön keresztül. Ez nagyon fontos ahhoz, hogy a virtuális eszközökre úgy tekintsünk, mintha azok valóban egy különálló eszközt képeznének. Az adatátvitelre a lehetőség úgy adódik, ha a két virtuális eszközhöz rendelt fizikai portokat összekötjük. Ez nem direktbe történik, hanem minden esetben tűzfalakon vagy egyéb biztonsági eszközön keresztül történik annak érdekében, hogy az összeköttetés szabályok által korlátozott és monitorozható legyen.

2.5. Szerverek pozícionálása

A jelenlegi infrastruktúrában több szerver is a belső hálózatra van kötve. A belső hálózatra kapcsolódnak a felhasználók is, ami biztonsági kockázatot jelent, mivel ugyanazon a hálózaton vannak és nincs közbeiktatva tűzfal, IPS vagy proxy, amivel monitorozható illetve szükség esetén korlátozható lenne a hozzáférés. Ez ellehetetleníti adott biztonsági eseményre történő elvárható időkereten belüli válaszadást.

A bevált gyakorlat azt diktálja, hogy mindig legyen legalább egy tűzfal réteg a felhasználók és a szerverek között, amivel jelentős biztonsági előrelépés érhető el, mivel a felhasználók számára csak azt biztosítjuk, amire valóban szükségük van ahelyett, hogy mindenhez korlátlan hozzáférésük lenne. Ha mégis úgy döntenénk, hogy ilyen korlátozásokat nem vezetünk be, még akkor is lehetőségünk van a hozzáférés monitorozásához és naplózásához, ami elengedhetetlen egy biztonsági esemény vizsgálatához. Amennyiben olyan biztonsági esemény következik be, mely beavatkozást igényel, akkor a tűzfal segítségével blokkolni tudjuk a forrás gép hozzáférését a szerverhez ezzel kiküszöbölve, hogy ez ne okozzon szolgáltatás kiesést a szerveren. Például egy fertőzött gép vagy botnet esetében.

A szerverek elhelyezésének kulcsa, hogy a megfelelő DMZ-be kell őket helyezni és azt az alapelvet kell követniük, hogy a kívülről elérhető szervereket a külső DMZ-be, míg a belső felhasználású szervereket a belső DMZ-be kell helyezni.



8. ábra: Jövőbeli hálózati topológia

Felhasználói kapcsolatok

Ahogy a szerverek esetében említésre került, mivel a DMZ-k ugyanazon az eszközön helyezkednek el, ezért elméleti lehetőség van áthatolni a biztonsági infrastruktúra kikerülésével a belső és külső DMZ-ken. Ez hatalmas biztonsági kockázat, mivel illetéktelen hozzáférés biztosíthat a DMZ-ben elhelyezett eszközökhöz, illetve az itt áramló adatfolyamokhoz. Ez többnyire hibás konfigurálás eredménye, ami lehet akár egy rosszul kialakított statikus forgalomirányítási parancs vagy mindkét külső és belső DMZ VLAN-ok ugyanazon fizikai porthoz történő véletlen hozzárendelése. Ez a Nexus VDC-ben soha nem fordulhat elő, mivel nincs a virtuális eszközök között átjárhatóság, anélkül, hogy közvetlen fizikai összeköttetést létesítenénk és ugyanazon portokat sem tudjuk több VDC-hez hozzárendelni. Azt gondolhatjuk, hogy MAC szűréssel jelenlegi konfiguráció esetén bizonyos védettségre teszünk szert, viszont ez sem védi a rendszert a vírussal fertőzött gépek ellen.

2.6. Üzemeltetési és szolgáltatási hálózatok

Értelemszerűen hálózatunkon minden eszköznek szüksége van felügyeletre. Tradicionálisan a különböző gyártói platformok számától függően az egy vagy több központi felügyeleti szerverrel történik. Az is előfordulhat, hogy rendszerünket külső szervezet is felügyeli és hibaelhárítást végez megfelelő VPN illetve Dial-in kapcsolatok segítségével. Ez nagy biztonsági kockázattal jár, mivel a felügyeleti eszközök nem minden esetben vannak elszeparálva a hálózat többi elemétől és lehetőség van azokról történő illetéktelen hozzáféréshez. Egy dedikált menedzsment VDC lehetővé teszi a menedzsment eszközök izolációját. Mindez kiegészítve privát VLAN-okkal drasztikusan növelhetjük a hálózat biztonságot. A privát VLAN-ok kialakítása úgy történik, hogy egy adott VLAN-hoz rendelt portokból bizonyos portokat arra korlátozunk, hogy azok csak egyetlen úgynevezett uplinkkel kommunikálhassanak. Ezeket a korlátozott portokat privát portoknak nevezzük. Tehát alapvetően egy pVLAN több privát portból és egyetlen uplinkből áll. Az uplink csatlakozhat akár egy tűzfalhoz, szerverhez, routerhez, szolgáltatói kapcsolathoz vagy egyéb központi erőforráshoz. Ennek előnyei, hogy annak ellenére, hogy a menedzsment eszközök ugyanazon a hálózaton vannak és IP címzésük ugyanabból a VLAN-ból kerül kiosztásra, ennek ellenére lehetetlen az egyik menedzsment eszközről a másikra ugrani. Ezzel a módszerrel biztonságosabb módon tudunk hozzáférést biztosítani külső felügyeleti szervezet számára egy adott VPN-en keresztül úgy, hogy mindezt tűzfal szabályokkal és ACL szabályokkal megtámogatjuk.