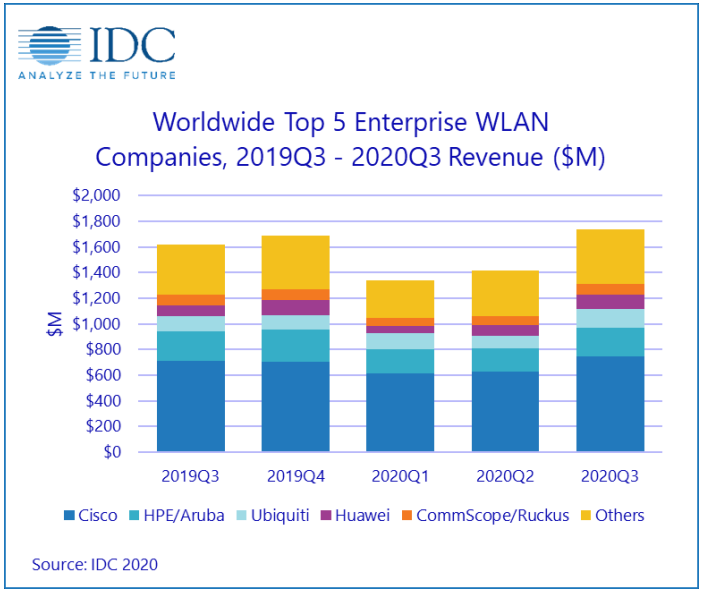
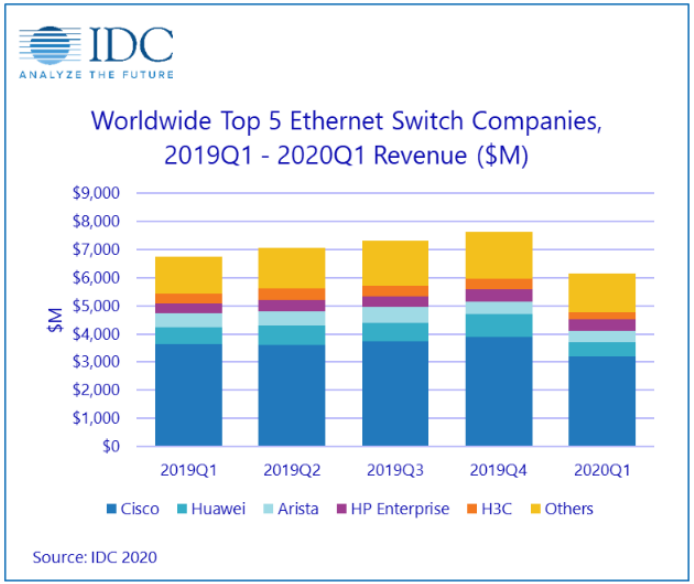
Hálózatok építése, konfigurálása és működtetése

Nagyvállalati hálózatok - Enterprise networks

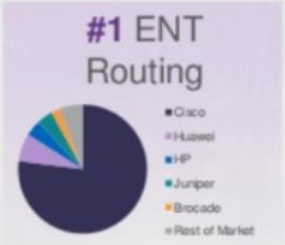
CISCO hálózatok

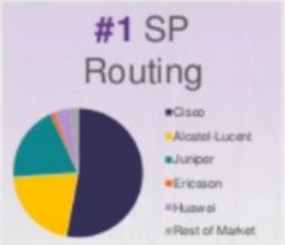
- Cisco eszközök a vállalaton belül

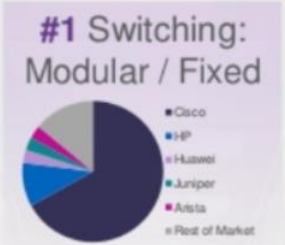


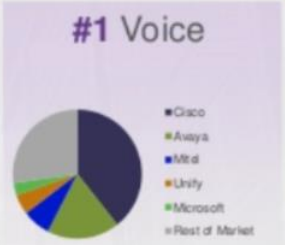


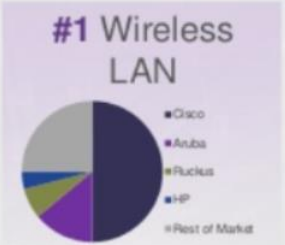
Cisco Competitive Advantage

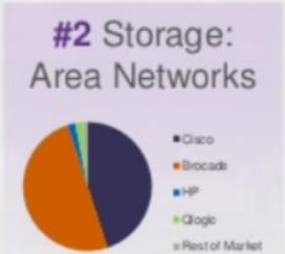


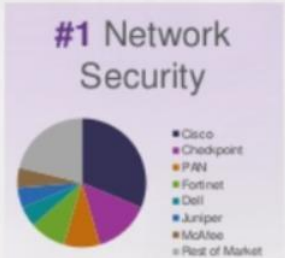


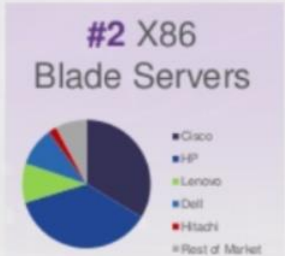


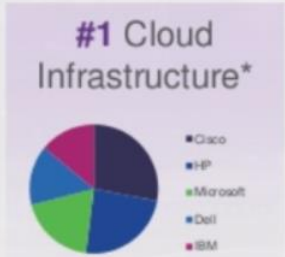












Source: Dell'Oro, Synergy, Infonetics, ACG; Q1'CY15 Market share data
Cisco Network Security share DOES include Sourcefire; Web Conferencing is SaaS
Competitors listed above are not the only competitors in these markets and share shown is relative share versus listed competitors
* Q4'CY14 Synergy data

CISCO Enterprise Campus

- Számítástechnikai infrastruktúra része
  - Hálózati szolgáltatások elérése
- Egy adott helyen elérhető hálózat
  - Lehet egy emelet vagy akár több épület is
- Nagy sebességű L2 és L3 rétegek

- Integrált elemek, amelyek szolgáltatások megvalósítását teszik lehetővé olyan felhasználók és eszközök között, akik ugyanazon a nagysebességű hálózathoz tartoznak
  - Vezetékes és vezetéknélküli adattovábbítás
  - Forgalom azonosítás és irányítás (biztonság)
  - Forgalom figyelés és menedzsment
  - Rendszer menedzsment

CISCO Enterprise Campus

- Campus hálózat követelmények
  - Globális elérhetőség
    - ötkilences rendelkezésre állás, valós idejű interaktív alkalmazások, gyors hibaelhárítás
    - Kevesebb, központosított adat. Hálózati elérés minden üzleti folyamatban
    - 7x24x365-ös működés
  - Együttműködések, valós idejű kommunikáció
  - Védekezés a támadások ellen
  - Gyors változáskövetés
    - Az eszközöket adaptálni kell a változásokhoz
    - Gyorsabb, egyszerűbb frissítések, módosítások
    - Új hálózati protokollok (pl. IPv6 megjelenése)
  - Következő generációs alkalmazások növekvő igényei
    - Multimédia, interaktív HD video
  - Heterogenitás
    - Partner és vendég hálózatok
    - Különböző eszközök támogatása

CISCO Enterprise Campus

- Hálózati tervezés
  - Rendelkezésreállás
  - Biztonság

  - Optimális erőforrás használat
  - Teljesítmény

  - Kritikus alkalmazások
  - Sokféle igény, sokféle forgalom

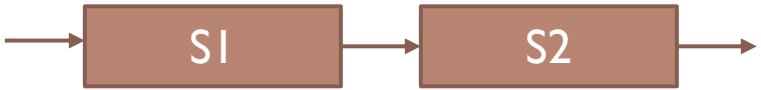
Rendelkezésreállás

Rendelkezésreállás

- MTBF: Mean Time Between Faliure
- MTTR: Mean Time to Repair

SLA: Service Level Agreement

- Rendelkezésre állás (Availability): $\frac{MTBF}{MTBF+MTTR}$
- Soros esetben (mindkét komponensre szükség van)
  - A_S: $A_1 \times A_2$



- Párhuzamos esetben (Csak akkor áll, ha mindkettő áll)
  - A_S: $1-(1-A_1) \times (1-A_2)$

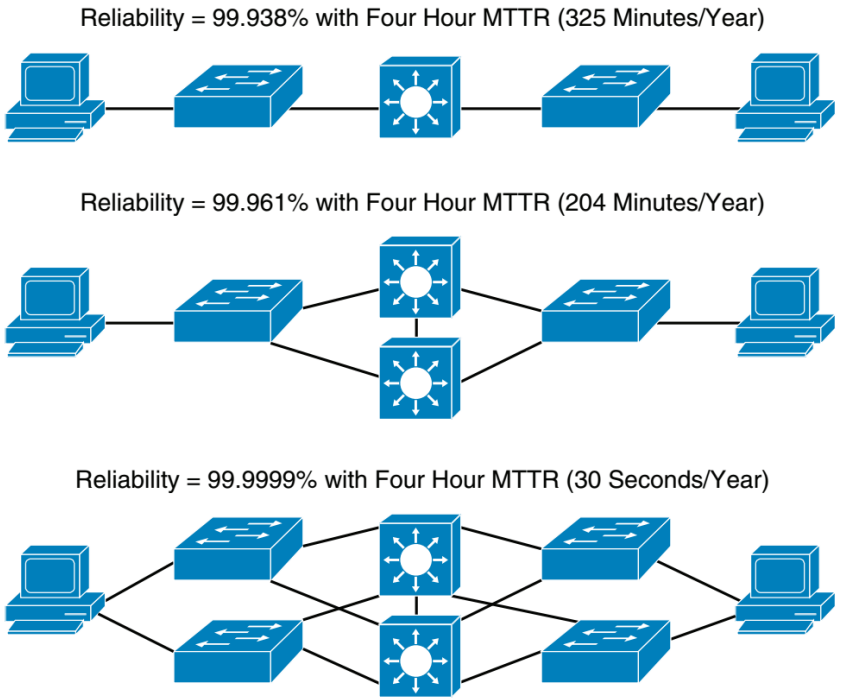
MTBF és MTTR értékek

- Cisco példa

- Catalyst 4500 datasheet

Part Number	Maximum Rated Power (W)	Rated MTBF (Hours)
WS-C4503-E	60	1,064,279
WS-C4506-E	120	710,119
WS-C4507R+E	135	248,630
WS-C4510R+E	200	179,714

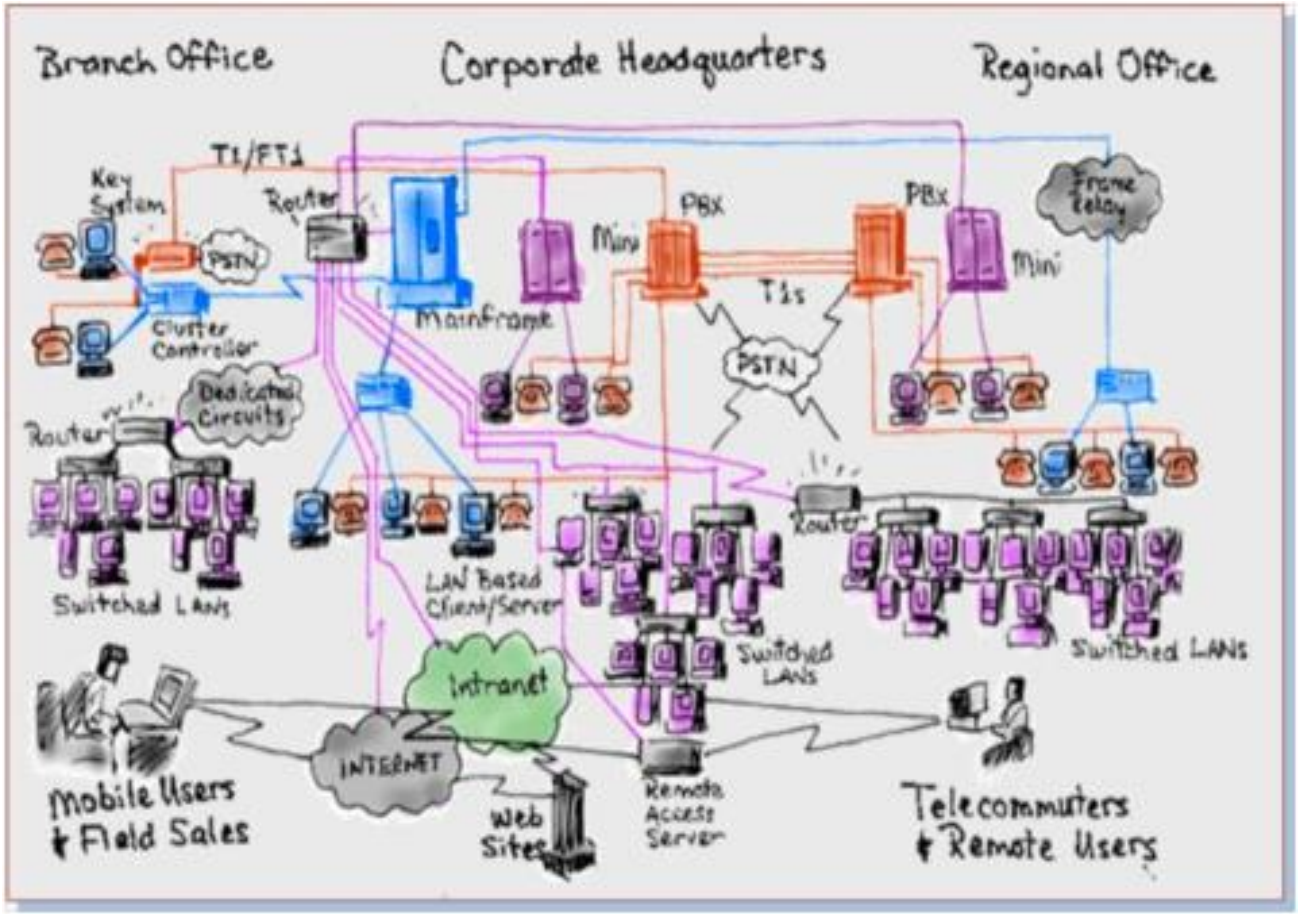
120 év



Defects per Million (DPM)

- A hiba hatása a felhasználó szemszögéből
  - Felhasználói élmény mérése
  - DPM: $\frac{\sum(\acute{e}rintett\ felhaszn\acute{a}l\acute{o}k\ sz\acute{a}ma \times kiesett\ id\H{o})}{\ddot{O}sszes\ felhaszn\acute{a}l\acute{o} \times teljes\ szolg\acute{a}ltat\acute{a}si\ id\H{o}} \times 10^6$
- Szintén fontos metrika, a maximális kiesés mértéke

Felépítés


Branch Office
Corporate Headquarters
Regional Office
T1/FT1
Key System
PSTN
Router
Cluster Controller
Mainframe
Mini
PBX
T1s
PSTN
PBX
Mini
Frame Relay
Dedicated Circuits
Router
Switched LANs
LAN Based Client/Server
Router
Switched LANs
Switched LANs
Intranet
INTERNET
Web Sites
Remote Access Server
Mobile Users & Field Sales
Telecommuters & Remote Users

Hierarchia és modularitás

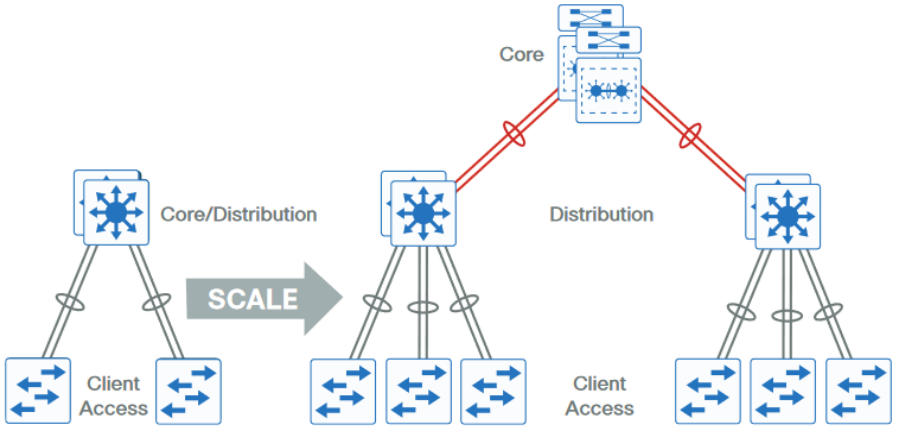
- Komplex rendszerek
  - Moduláris komponensek …
  - … hierarchikusan felépítve

Külön-külön tervezhetőek
Részben független elemek
Egyszerűbb menedzsment

Minden elemnek meghatározott szerepe van
Meghatározott funkciók és szolgáltatások

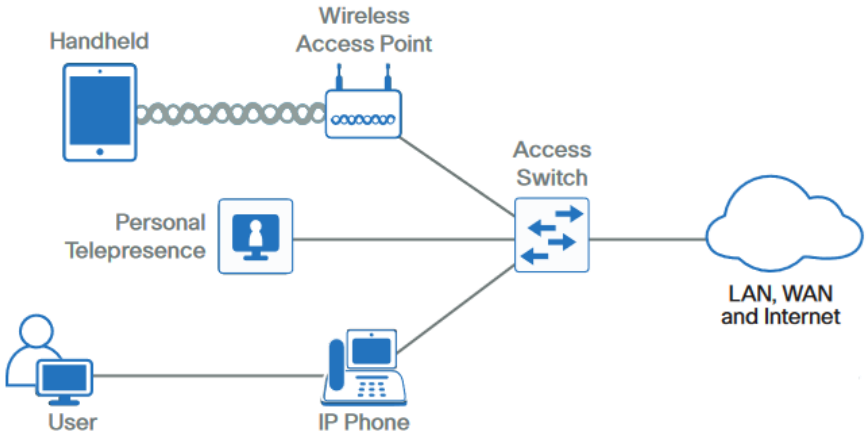
Campus hierarchia

- 3 szintű hierarchia
  - Lehet kevesebb is és több is
  - **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
  - **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
  - **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása



Access (hozzáférési) réteg

- **Felhasználó gépek, végpontok csatlakozása**
- Vezetékes vagy vezetéknélküli kapcsolat
  - Nagy sávszélességű kapcsolat
  - Több alhálózat (logikai szétválasztás)
    - Teljesítmény, biztonság, menedzsment
- Biztonságos, hibatűrő működés
  - Magas rendelkezésreállás
  - Védekezés az emberi hibák és rosszindulatú támadások ellen
  - Hitelesített szolgáltatások és felhasználók
- Megkülönböztetett forgalmak



Hozzáférési réteg feladatai

- A legszélesebb funkciókínálatot mutató réteg
  - Konfigurálás, feltérképezés
  - Biztonsági szolgáltatások
  - Hálózati azonosítás
  - Alkalmazás felismerő szolgáltatások
  - Intelligens hálózat irányítási szolgáltatások
  - Fizikai infrastruktúra szolgáltatások (PoE)

- A hálózat és az eszközök határa
  - Biztonság, QoS, házirend feladatok

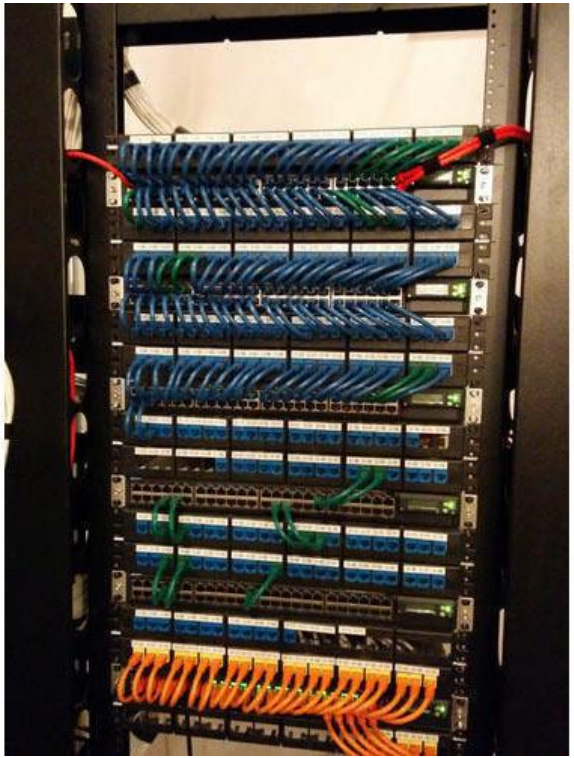
Hozzáférési réteg eszközei

- Felhasználói eszközök
  - Munkaállomások, VoIP berendezések, hozzáférési pontok, kapcsolók

- Gigabit Ethernet switch
  - Biztonsági megoldások, monitorozás, PoE
  - „Stackable”
  - 2-5 Gpbs sebesség
  - Pl: Cisco Catalyst 2960-X, Catalyst 3850, HP 5500

Hozzáférési réteg eszközei

- Rack szekrény



Core (központi) réteg

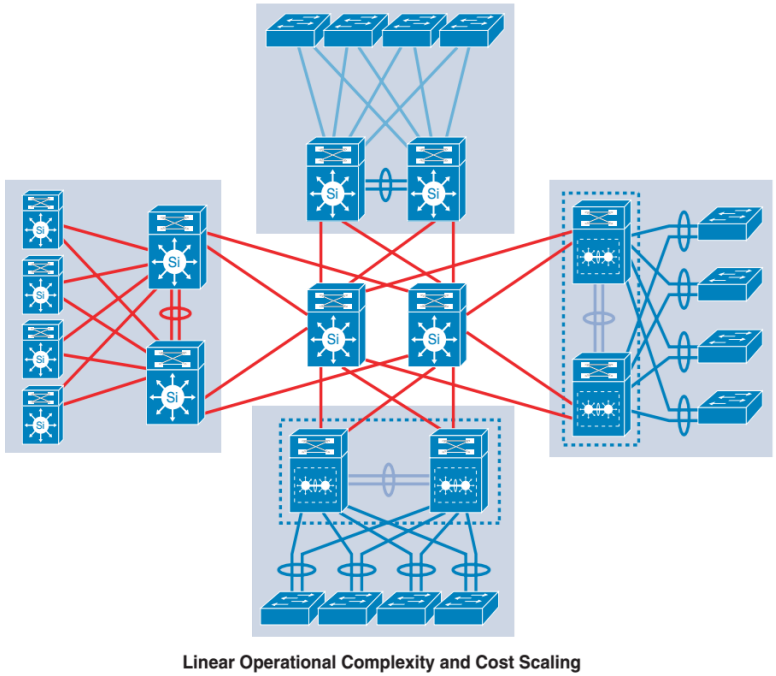
- **Állandó összeköttetés az egész campus számára**
- A legegyszerűbb, de egyben a legkritikusabb réteg
  - Always-on, 7x24x365

- Nagyon szűk szolgáltatáskör
  - Nincsenek felhasználók
  - Nincsenek házirendek
  - Kizárólag Layer 3 kapcsolatok! (Nincs switching)

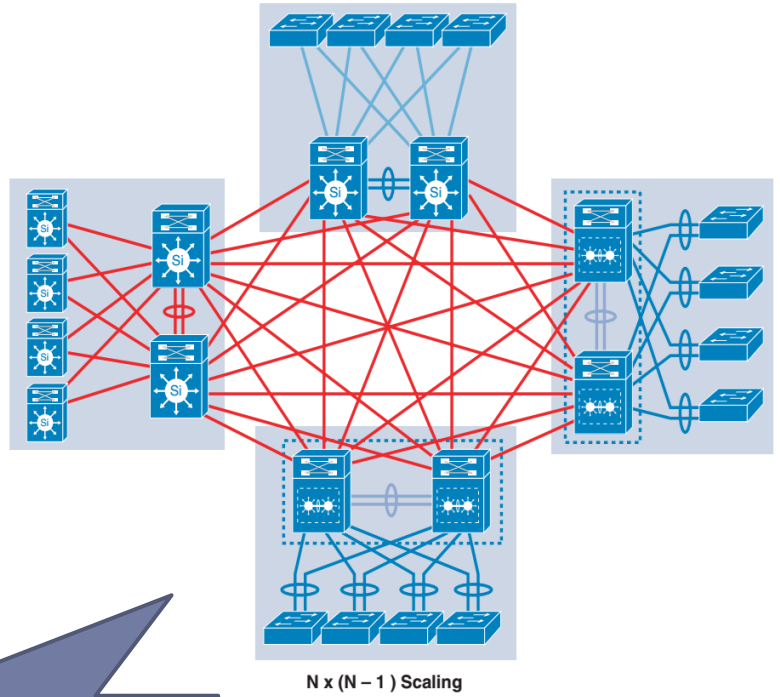
Központi réteg

- REDUNDANCIA! Nagyon fontos, hogy bármely eszköz kiesése esetén maradjon a működés
  - Tervezett bővítések, cserék
- Feladata, hogy a campus más moduljainak aggregálása

Központi réteg nélkül



VS

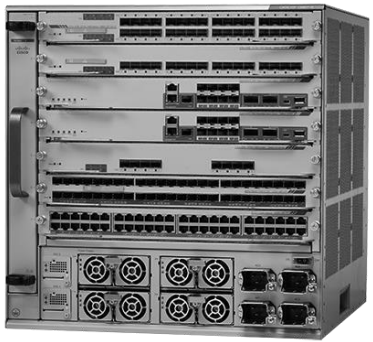


Több kapcsolat, költségesebb is

Központi réteg eszközei

- 10/40/100 Gb Ethernet
- Redundancia

- Pl: Cisco Nexus 7700, Catalyst 6800, HP 7500



Distribution (elosztási) réteg

- Irányítási határ
- Szolgáltatás és szabályozás réteg a hozzáférési és a központi réteg között
  - Kapcsolódás a hozzáférési réteghez
    - Aggregálja a hozzáférési pontok forgalmát
  - Kapcsolódás a központi réteghez

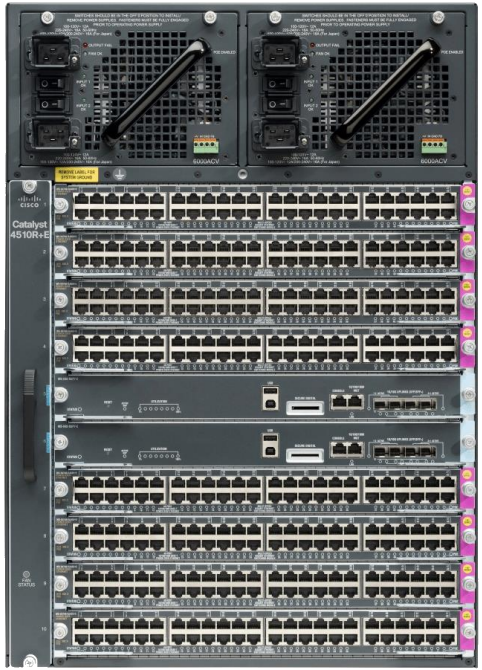
- Szabályozás
  - A helyi forgalom maradjon a helyi hálózaton
  - Forgalomszűrések, forgalomfelügyelet
    - Hozzáférés vezérlés
    - Támadás, hiba esetén hibatartomány korlátozás

Komplexitás, rendelkezésreállás

- A hozzáférési réteg
  - Csökkenti a komplexitást
    - Kapcsolatok számának csökkentése
    - Konfigurálás komplexitásának csökkentése
  - Növekedő rendelkezésreállás
    - Redundancia. Redundáns táp, modulok
    - Másodperc közeli helyreállás

Elosztási réteg eszközei

- Cisco Catalyst 3850, Catalyst 4500 sorozat
  - Többszáz Gbps
  - Magas szintű rendelkezésre állás képesség
  - Skálázhatóság
  - Intelligens szolgáltatások vezetékes és vezeték nélküli hozzáféréshez



Hibakezelés

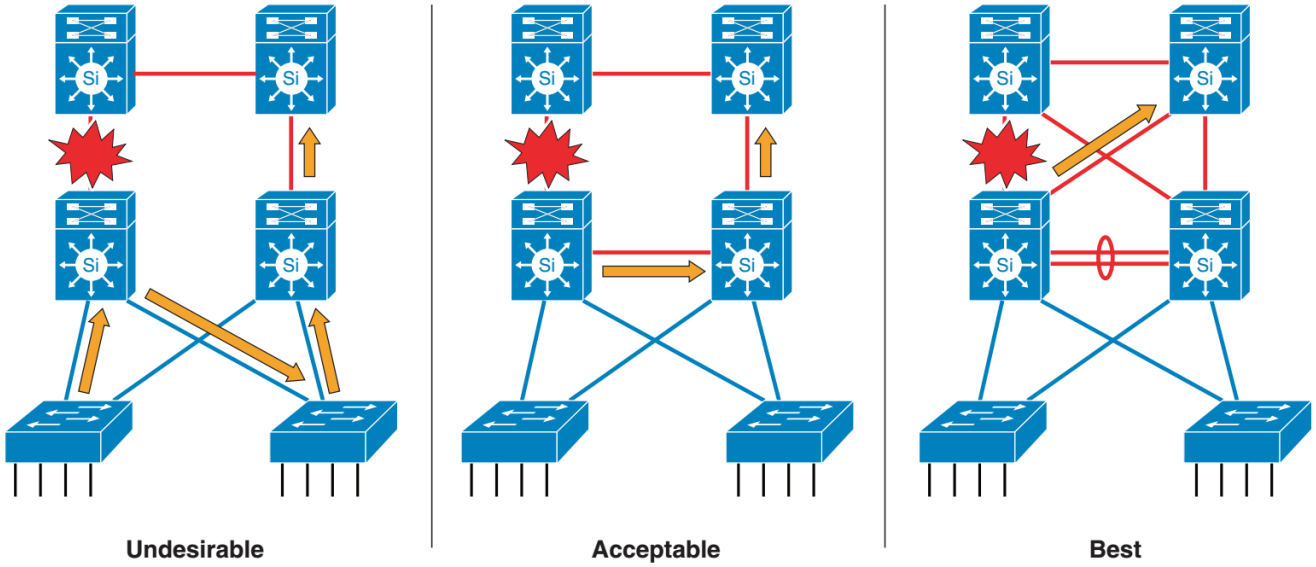
Hibakezelés a 3 rétegű modellben

- Meghatározott funkciók a rétegekben
- Pl. hiba kezelés

központi

elosztási

hozzáférési

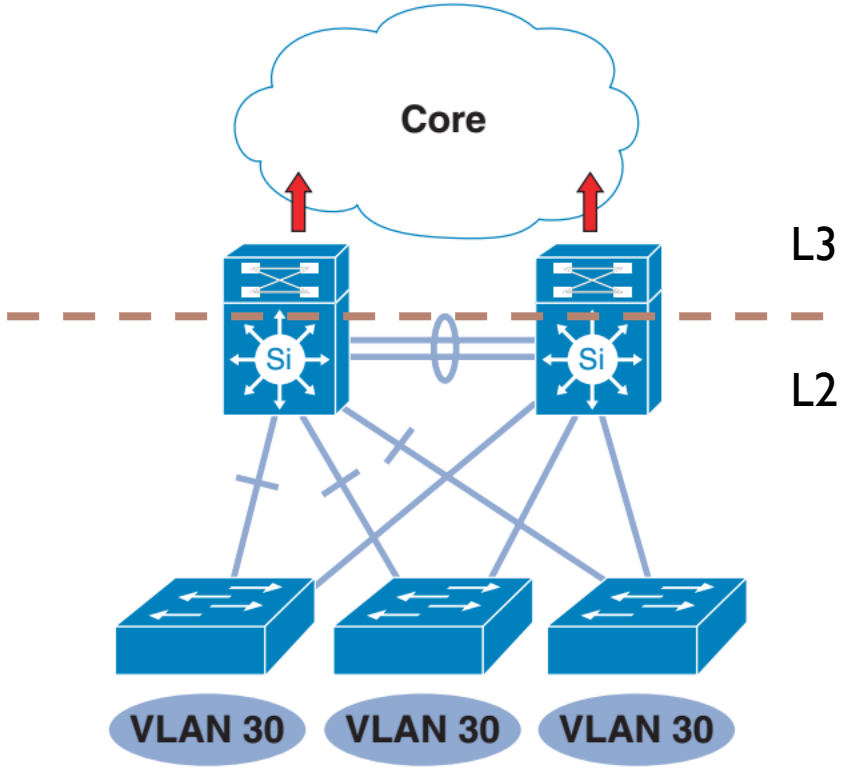


Hozzáférési-elosztási réteg

- Gyakorlati megvalósítása
  - Többlépcsős (multi-tier) megoldás
  - „routed access”
  - Virtuális kapcsoló
- Minhárom megoldásnál a topológia azonos, a kábelezés hasonló
  - Különböző beállítások, képességek

Többlépcsős hozzáférési-elosztási réteg

- Hozzáférési réteg: L2
- Elosztási réteg: L2 & L3
- VLAN trönkök
  - Akár több switchen keresztül
- FHRP
  - First-hop redundancy protocol
  - Konvergencia: 900ms-9mp
- STP protokoll
  - Hurokmentesítés
  - Lassú konvergencia (akár 50 mp)



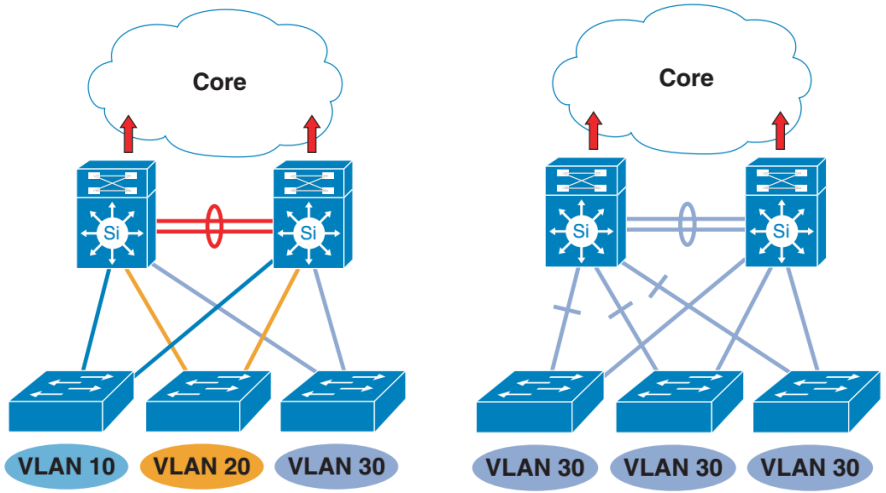
FHRP: First-hop redundancy protocol

- Rendelkezésreállás növelése
  - Beugrás a kieső router helyére (de nem csak router)

- Hot Standby Router Protocol (HSRP)
  - Prioritások szerinti ARP válasz
- Virtual Router Redundancy Protocol (VRRP)
  - A hoszt alapértelmezett routere egy csoportból kerül ki (virtuális router)
- Gateway Load Balancing Protocol (GLBP)
  - Terhelésmegosztásos IP cím megosztás (súlyozás)
  - Az ARP válaszoknál különböző virtuális MAC címek kerülnek vissza
- Common Address Redundancy Protocol (CARP)
  - Egy IP cím megosztása több gép között (master/slave)
  - Terhelésmegosztás is lehetséges

Többlépcsős variációk

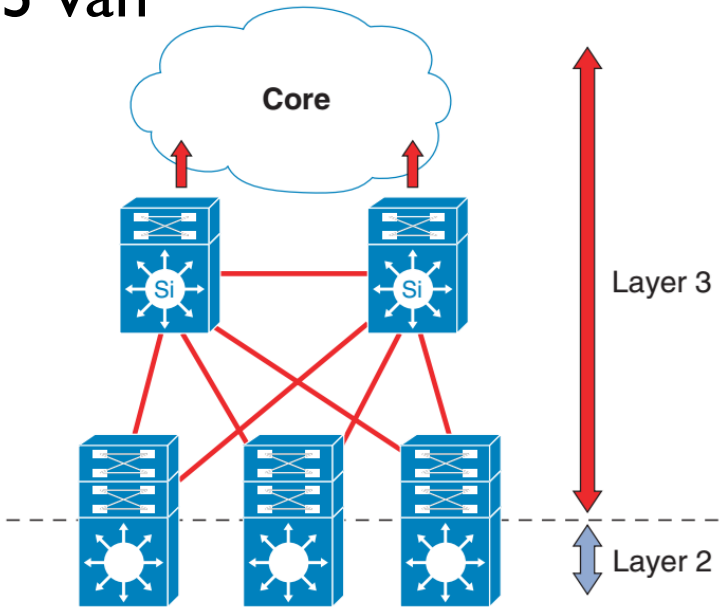
- Hurokmentes (V) és hurkos változatok
  - A hurok eltávolítása előnyös
    - Terhelésmegosztás
    - STP függőség csökkentése



Hurokmentes Hurkos

Routed access

- A hozzáférési rétegben már elérhető a L3
- Az elosztási rétegben már csak L3 van
- Az elosztási réteg funkciói a hozzáférési réteghez kerülnek
  - Alapértelmezett átjáró, VLAN
  - Nincs szükség az FHRP protokollokra, lokális átjárók



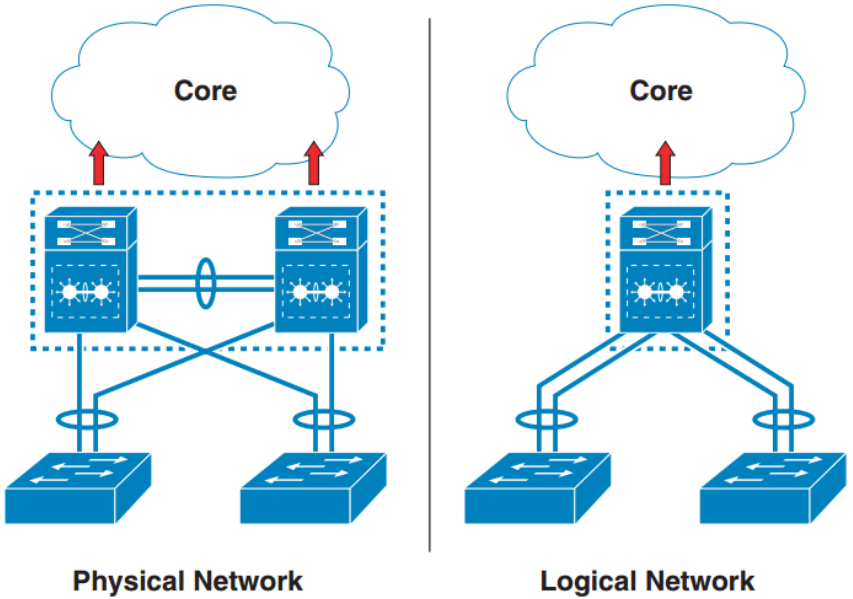
Routed access előnyök, hátrányok

- Routing protokollok
  - Konvergencia: < 200ms
  - Reroute hiba esetén
- Könnyebb hibakeresés, ismert szerszámok
  - Ping, traceroute, ip route
- Egyetlen kontroll protokoll, nincs FHRP

- Ugyanakkor vannak korlátok is
  - A VLAN nem terjedhet át másik kapcsolóba

Virtuális kapcsoló (Virtual Switch System - VSS)

- Régi megközelítés:
  - Redundáns elosztási réteg kapcsolók és protokoll, amely meghatározza az aktívat és vált hiba esetén
- Új megközelítés:
  - A redundáns elosztási réteg kapcsolók egyetlen logikai kapcsolót alkotnak



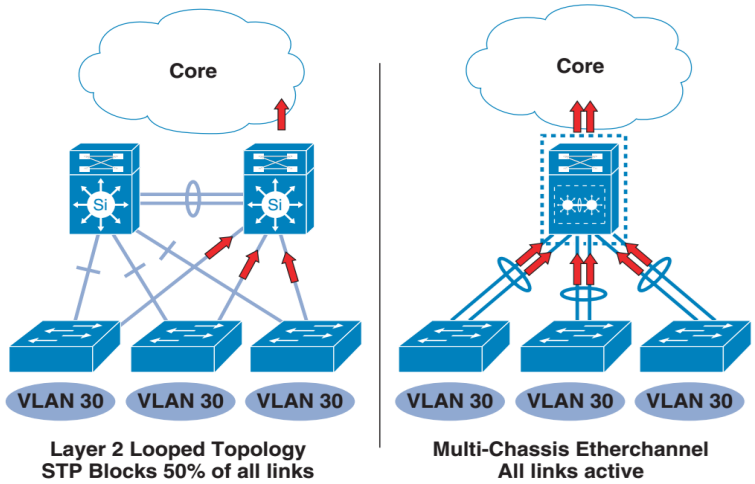
Virtuális kapcsoló előnyök

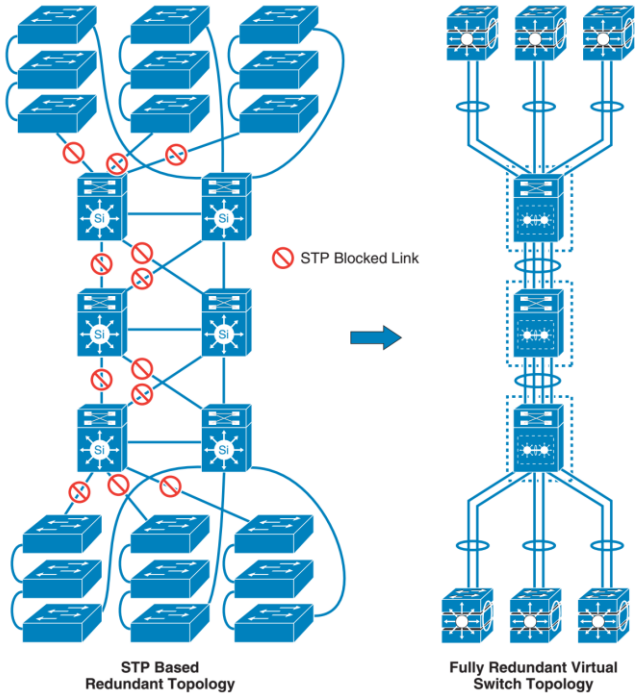
- **Nincsenek hurkok a (logikai) kapcsolatban**
  - STP maradhat, mint tartalék megoldás
- Egyszerűsödik a topológia
- Terhelésmegosztás flow alapon
- Hiba esetén gyors váltás, nincs szükség megvárni az STP-t, vagy hasonló protokollt
- A VLAN több hozzáférési kapcsolóra is kiterjedhet

- A technológia nincs korlátozva csak a hozzáférési / elosztási rétegre

Virtuális kapcsolók vs. STP

- Nő a teljesítmény





Összehasonlítás

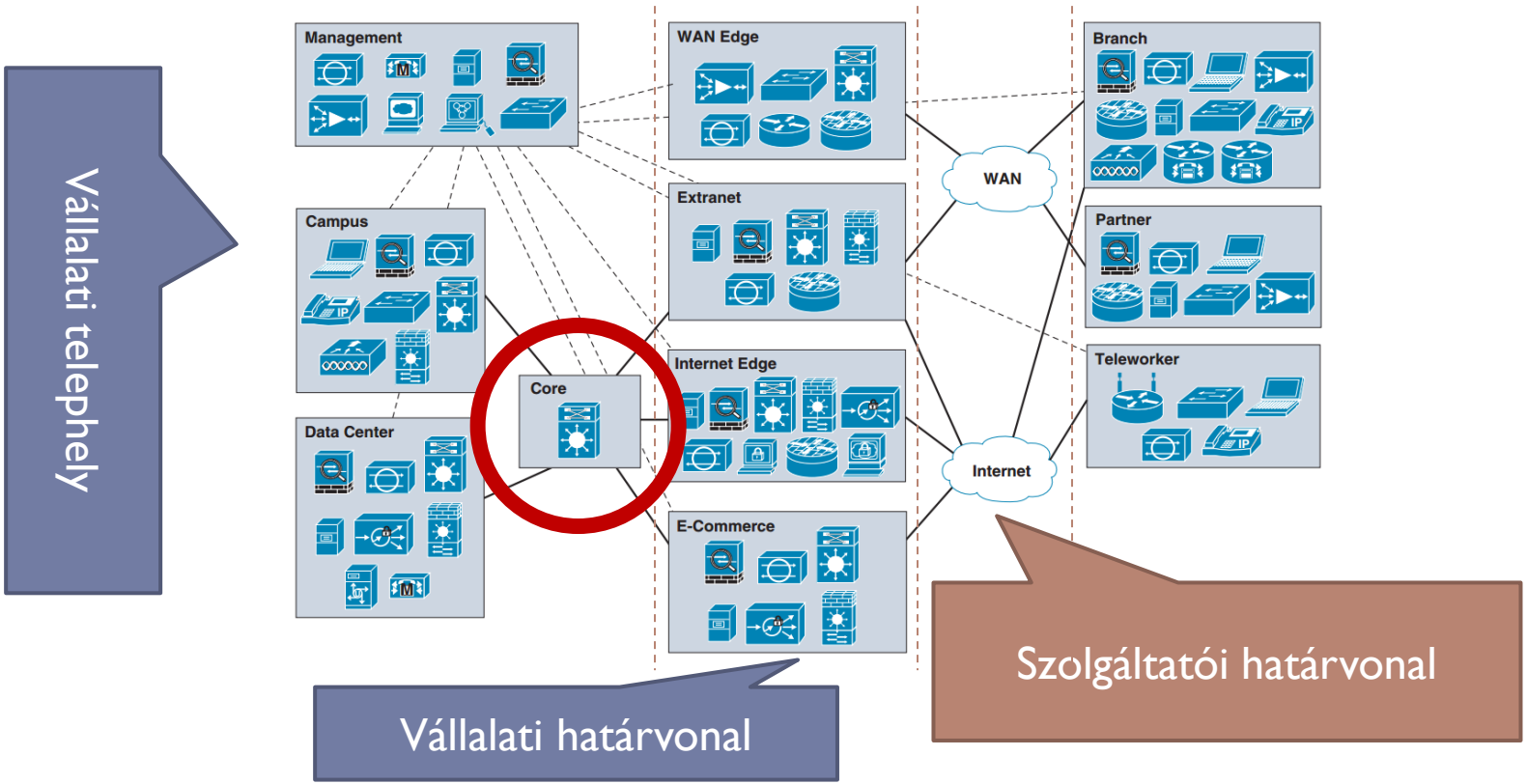
	Többlépcsős Multitier Access	Routed Access	Virtual Switch
Protokollok	STP	Routing, pl: OSPF	(PAgP, LACP)
STP szükség	Szükséges	Nincs	Nincs, de tartaléknak jó
Hibaelhárítás	STP és FHRP	Re-routing	Multichassis EtherChannel (MEC)
VLAN átívelése kapcsolón	Támogatott, de nem ajánlott	Nincs	Támogatott
L2 és L3 határa	Elosztási réteg	Hozzáférési rétes	Elosztási réteg (akár hozzáférési réteg is)

Összehasonlítás folyt.

	Többlépcsős Multitier Access	Routed Access	Virtual Switch
Protokollok	STP	Routing, pl: OSPF	(PAgP, LACP)
FHRP	Szükséges	Nincs	Nincs
Terhelésmegosztás	Alhálózat vagy hoszt alapon	Flow alapon	Flow alapon
Konvergencia	900ms-50mp	50-600ms	50-600ms

CISCO Enterprise Architecture

CISCO Enterprise Architecture (CEA)



Nagyvállalati architektúra

Központi réteg

Enterprise Core

- Fenyegetések
  - Szolgáltatás akadályozás (DoS és DDoS támadások)
  - Jogosulatlan hozzáférés és ebből következő további támadások
    - Jogosulatlan felhasználók, jogosultság megemelése, hozzáférés védett infrastruktúrához, routing protokoll támadások
  - Adat hozzáférés
    - Adatlopás, közbeékelődéses támadások (MITM)

Enterprise Core

- Védekezések
  - Redundancia: DoS/DDoS elleni védekezés, routing protokoll támadások ellen
  - Felesleges szolgáltatások kikapcsolása: DoS/DDoS elleni védekezés, jogosulatlan hozzáférés ellen, behatolások ellen
  - Jelszavak védelme, naplózás, hitelesítés (SNMP): jogosulatlan hozzáférés ellen, behatolások ellen
  - Hozzáférési listák felállítása: DoS/DDoS elleni védekezés, jogosulatlan hozzáférés ellen, behatolások ellen
  - Router hitelesítése: DoS elleni védekezés, jogosulatlan hozzáférés ellen, routing protokoll támadások ellen
  - Control Plane Policing (CoPP): Minden támadás ellen

Control Plane Policing (CoPP)

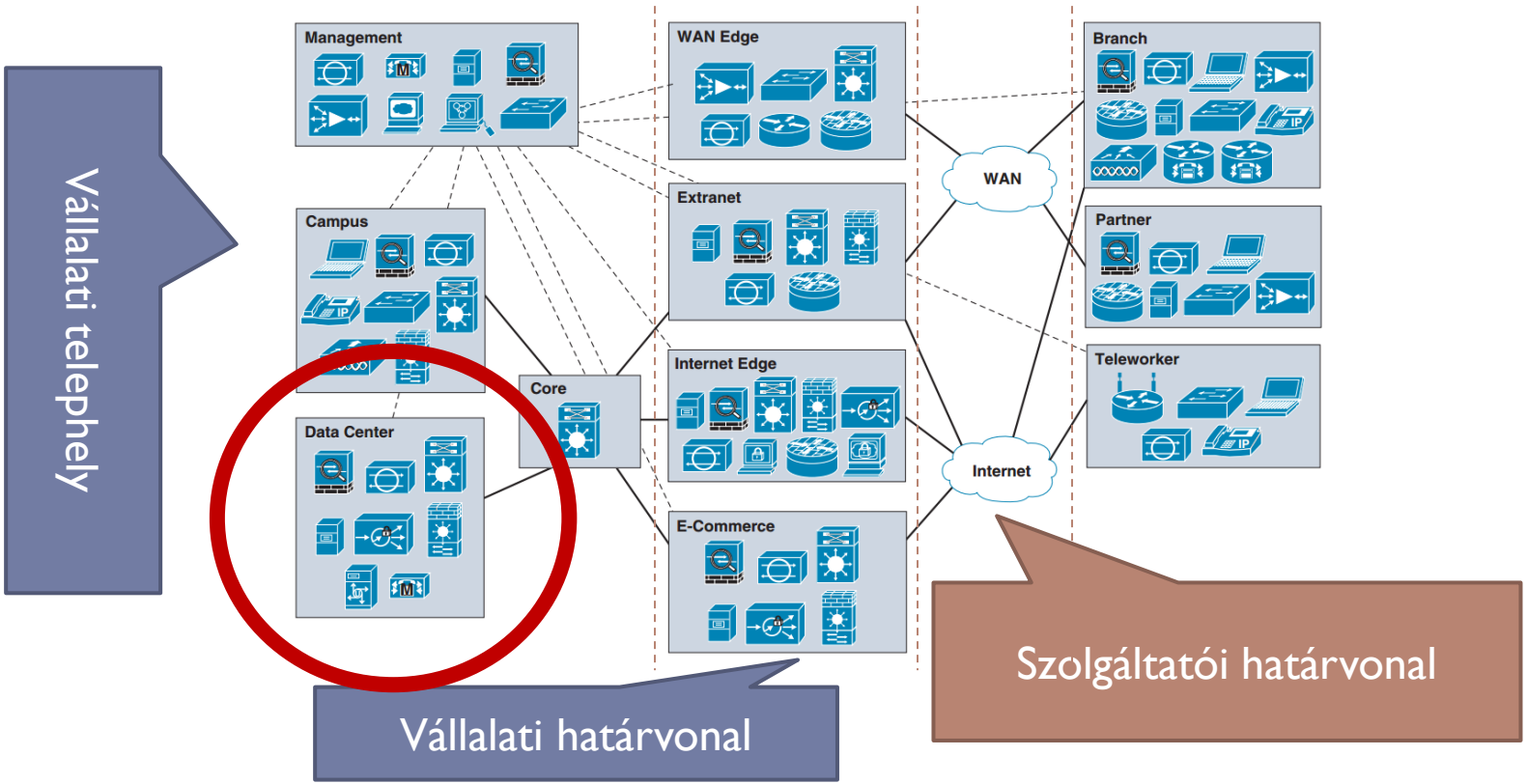
- A menedzsment és irányító sík (management, control plane) védelme az adat sík elárasztása esetén
  - Prioritások
  - Hozzáférési listák
  - Szűrés, rate limit

- Stabil routing, elérhetőség

Nagyvállalati architektúra

Adatközpont

CISCO Enterprise Architecture (CEA)



Intranet Data Center

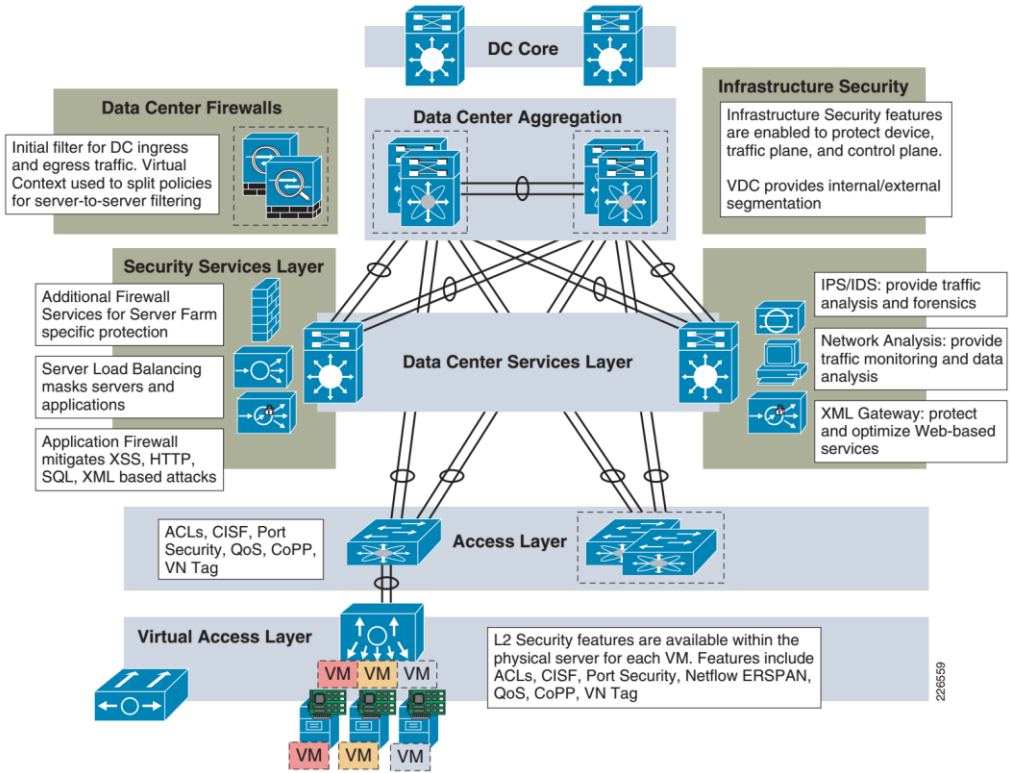
- A kritikus alkalmazások és adatok zöme
  - Jellemző a virtualizáció
  - Az egyik alapvető követelmény a biztonságos tervezés

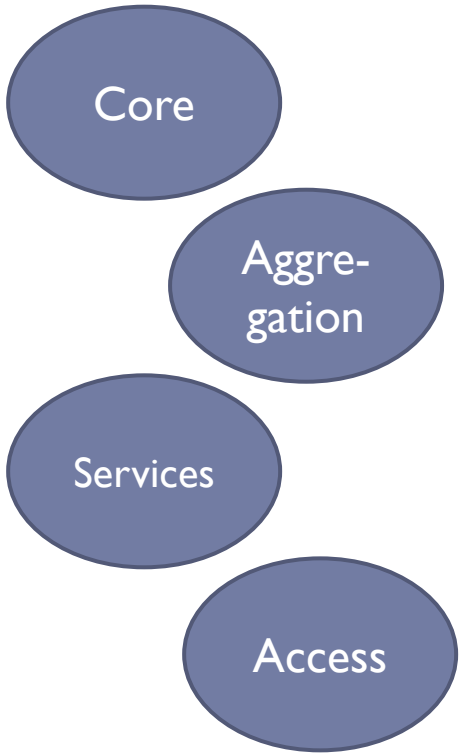
- Biztonság
  - Elszigetetlés (Isolation)
    - Tűzfalak, hozzáférési listák, VLAN-ok, virtualizáció, fizikai elszigetelés
  - Házirendek (Policy Enforcement)
  - Felügyelet (Visibility)

Data Center támadások

- Kiszolgálás főleg a belső hálózat felé
  - De védekezés kívülről jövő támadások ellen is
  - Főleg alkalmazási rétegben lévő támadások (HTML, SQL, XML, …)
- Támadási vektorok
  - Jogosulatlan hozzáférés (eszközhöz vagy adatokhoz)
  - Szolgáltatás megakadályozás
  - Adatvesztés
  - Adat módosítás

Data Center felépítése





Data Center Core

- Belépési pont az adatközpontba
  - Routing feladatok
  - Az adatközpont aggregációs rétegek kapcsolása
- Védekezés routing támadások ellen
  - Az összekötött eszközök (peer) hitelesítése
  - Routing szűrések
  - Naplózás

Data Center Aggregation

- Virtual Device Context (VDC)
  - Síkok (vezérlés, adat, menedzsment) virtualizációja
  - Logikai szétválasztás
- Tűzfalak
  - Megfelelő hely a tűzfalak elhelyezésére
    - Nagy teljesítményű tűzfalak (10 Gbps forgalom megfigyelése)
    - Állapotok figyelése, Layer 2 forgalom
  - A tűzfal szintén virtualizálható, több logikai tűzfalra

Data Center Services

- Skálázhatóság
- Biztonság
- Védelem
  - Alkalmazás tűzfalak, tűzfalak
  - Behatolás jelző/megelőző rendszerek (Intrusion Detection/Prevention System)

A titkosított adatforgalom nem megfigyelhető, ezért itt már nincs titkosítás: SSL-proxy

Data Center Services

- Webes alkalmazások biztonsága
  - Tűzfal – Web Application Firewall (WAF)
    - Védelem a megszemélyesítés, adatlopás, szolgáltatás megtagadás, csalás ellen
    - Támadások: XSS (Cross Site Scripting) támadás, SQL injektálás, Buffer overflow, Cookie tampering, DoS
  - Működés, mint reverse proxy

- Behatolás jelző rendszerek – Intrusion Prevention System
  - DPI – Deep Packet Inspection
  - Anomáliák figyelése

Data Center Access

- L2 kapcsolat a szerverfarmhoz
- Skálázhatóság a legalapvetőbb kritérium

- L2-re fókuszált védelem
  - VLAN technológia az adatutak szétválasztására
  - Hozzáférési listák (ACL) a jogosultságok ellenőrzésére
  - ARP-DHCP forgalom felügyelete
  - Port elárasztások megakadályozása

- Virtuális hozzáférési réteg
  - Logikailag a hozzáférési réteggel egyező

Catalyst Integrated Security Features (CIFS)

ARP-DHCP felügyelet

- DHCP snooping
  - A nem megfelelő DHCP forgalom eldobása
  - Összerendelések: MAC cím – IP cím - VLAN
- Dynamic ARP inspection
  - A nem megfelelő ARP forgalom eldobása
  - Statikus konfiguráció vagy DHCP snooping
- IP Source Guard
  - IP cím hamisítás (IP spoofing) ellen
  - Statikus konfiguráció vagy DHCP snooping

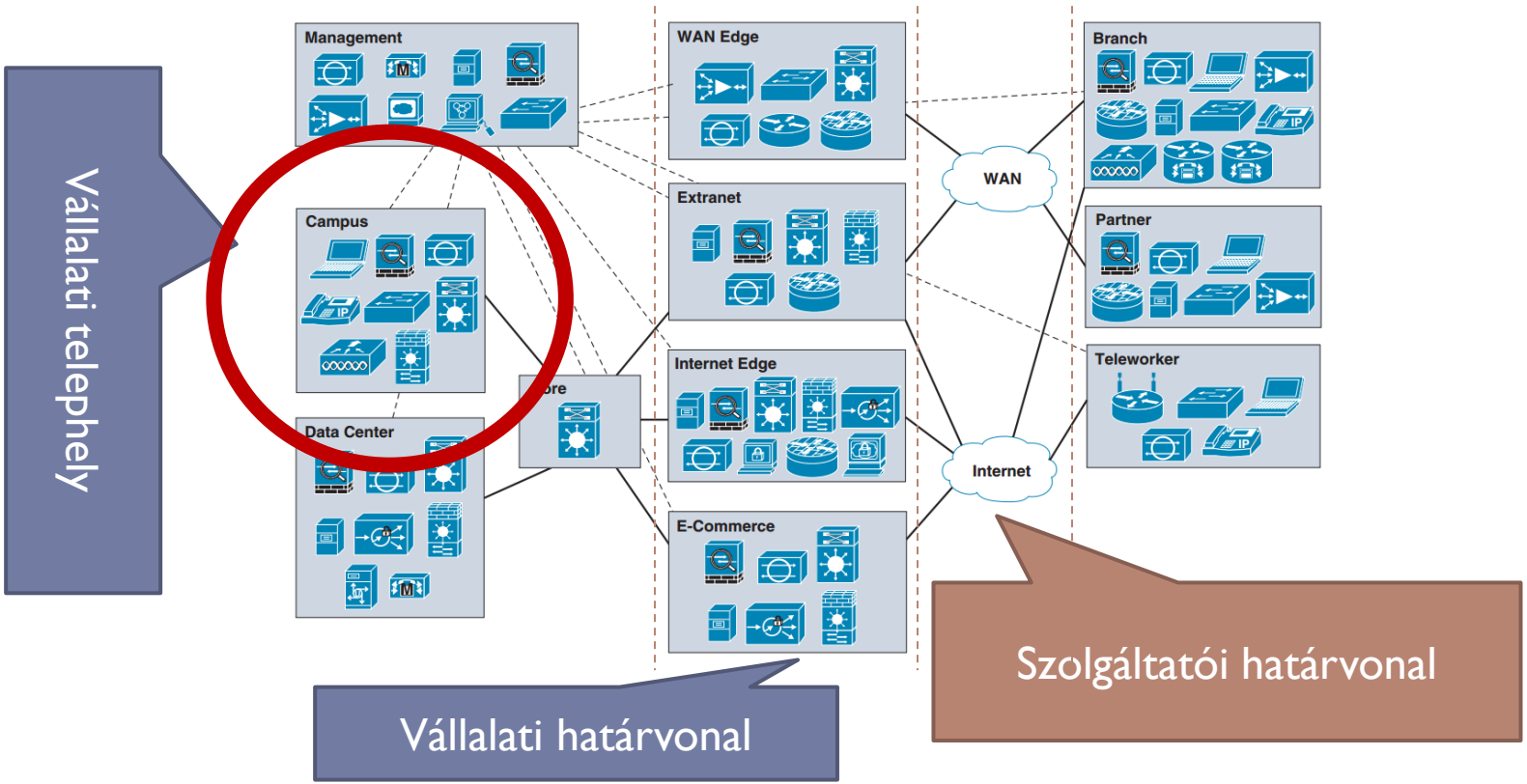
Virtuális hozzáférési réteg

- Virtuális gépek
  - Adott esetben a forgalom nem hagyja el a gazda gépet
    - Elszigetelés és megfigyelés nehézségei
  - Virtuális kapcsolók
    - Virtuális felügyelet és hálózati interfész
    - Házirend profilok az egyes virtuális interfészeknek
    - Beágyazott távoli port analizátor - Encapsulated Remote Switched Port Analyzer (ERSPAN)
      - Virtuális IDS/IPS szenzorok
      - Forgalom tükrözése forgalom analízis céljából

Nagyvállalati architektúra

Campus hozzáférési és elosztási rétegek

CISCO Enterprise Architecture (CEA)



Enterprise Campus – hozzáférési réteg

- A nagyvállalati felhasználók csatlakozása
  - Heterogén eszközök (munkaállomás, laptop, printer, VoIP telefon, …)
    - Nehezen karbantartható megfelelő biztonság (sérülékenységek, vírusok)
    - Hordozhatóságból adódóan vállalathoz bejutó problémák
      - A felhasználók hozzák be a támadást
  - Veszélyeztetik az egész nagyvállalatot

Végpontok elleni támadások

- Védekezés a végponton
  - Védekezést ismert támadások ellen
    - Vírusok, férgek. Védekezés szignatúrák alapján
  - Védekezés 0day és még nem javított támadások ellen
  - Házirendek betartatása
- Hoszt alapú IDS

- Nem csak a végpontokat, hanem az infrastruktúrát is védeni kell

Infrastruktúra védelme

- Dedikált menedzsment interfészek, Out-of-Band (OOB) menedzsment hálózat
- Elérhető portok, kommunikáció, hozzáférés korlátozása
- Hitelesítés, jogosultság, naplózás (AAA)
- Routing védelme
- Redundancia biztosítása
- Hálózat felügyelet, eszközök felügyelete
- Hálózati eszközök elérése hozzáférési lista alapján (ACL)
- L2 védelem (DHCP, ARP, MAC, …)

Enterprise Campus – elosztási réteg

- Infrastruktúra védelme
- Végpontok védelme

- Behatolás felismerő rendszerek (IDS/IPS)
  - Adatútba helyezve (inline)
    - Azonnal hatás, a forgalom szűrése
    - Teljesítmény szempontjából kritikus
  - Lehallgató módban (promiscous)
    - Távoli szenzorok küldenek adatot (Switched Port Analyzer – SPAN, RSPAN)
  - Terhelésmegosztással is dolgozhatnak
    - Akár virtuális kapcsolók esetén is

IDS forgalom szimmetria

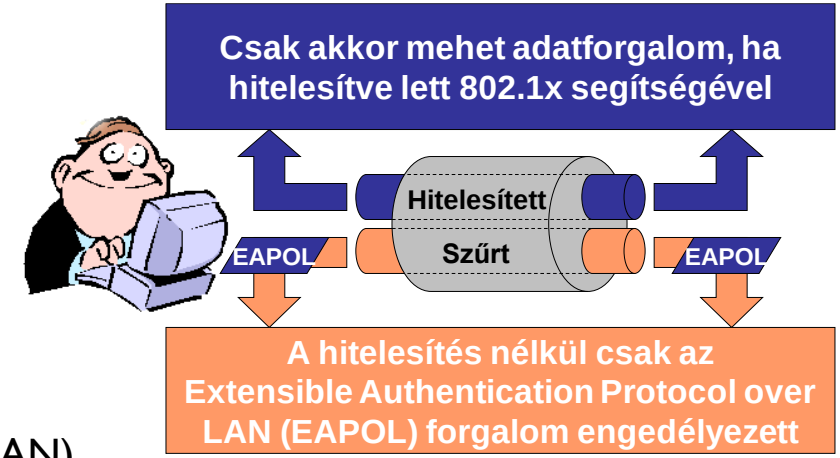
- A felismerés szempontjából kritikus, hogy az IPS szimmetrikus forgalmat lásson (mindkét irány)
  - A forgalom másolása minden IPS-re
    - Nagy forgalom esetén lehetetlen
  - A forgalom egyetlen kapcsolóra terelése
    - Meghibásodás esetén nagy probléma (Single Point of Faliure)
  - A forgalom irányítása (Policy Based Routing), hogy a két irány egyetlen kapcsolón menjen keresztül
    - Hatásos, de bonyolult lehet
  - A terhelésmegosztás irányítása (sticky load balancing), hogy a két irány egyetlen IDS-es menjen keresztül
    - Hatásos, de plusz eszközt igényel

Network Access Control (NAC)

- A hálózati elérés szabályozása
  - Különböző jogosultságú felhasználók
    - Dolgozó, szerződéses külsős, partner, vendég, …
  - A hálózat elérhető az egész campus területén
    - Ma már NEM a fizikai védelem (nincs hálózat) a jellemző
  - Személyes vagy szerepkör szerinti azonosítás
  - Megfelelés a biztonsági előírásoknak
    - Megfelelő biztonsági szoftverek, patchek
    - A nem megfelelő eszközök karanténba helyezése

Végpontok csatlakozása

- Csatlakozás hitelesítése
  - IEEE 802.1X – Port-based Network Access Control
    - Felhasználó hitelesítése különböző módszerekkel
  - MAB - MAC Authentication Bypass
    - Hitelesítés MAC cím alapján
  - WebAuth
    - HTTP alapú kommunikáció
    - Hitelesítő oldal megjelenítése
- Hitelesítési sorrend (probléma esetén)
  - 802.1X -> MAB -> WebAuth
  - Változtatható, tiltható
- Újrahitelesítés lehetősége
- Hitelesítés nélkül külön hálózatra kerülhet (VLAN)



Identity-Based Networking Services

- Hitelesítési szintek
  - Elő hitelesítés (hitelesítés előtt)
    - Általában zárt port
    - Lehet korlátozott hozzáférés is. Vannak eszközök, amelyek a hálózatról élednek fel
      - DHCP, TFTP forgalom
  - Sikeres hitelesítés
    - Utó hitelesítés: VLAN-ba sorolás
  - Sikertelen hitelesítés
    - Hasonló helyzet az elő hitelesítéshez

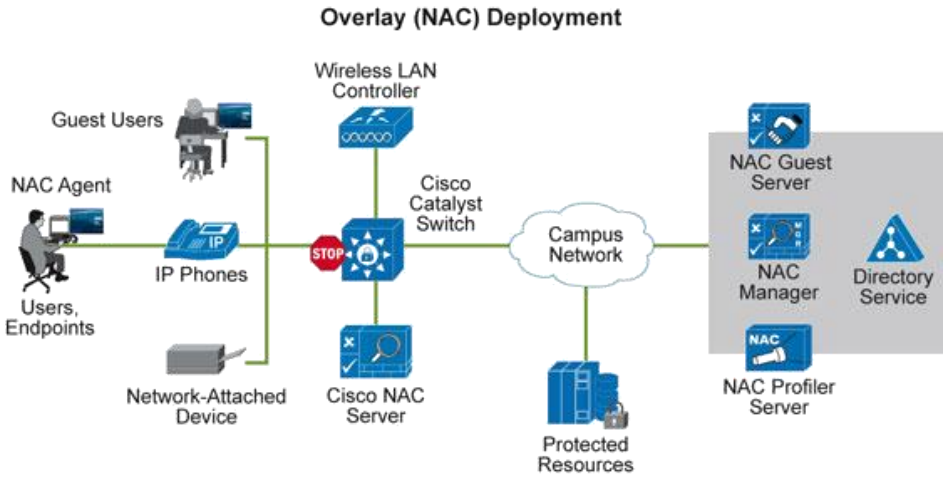
- Összeköttetés
  - Single host: Egyetlen gép a port mögött
  - Multi domain: Egy VoIP telefon (VoIP VLAN) és egy számítógép (adat VLAN)
  - Multi auth: Egy VoIP telefon (VoIP VLAN) és több számítógép (adat VLAN)
    - Virtuális gépek esetén

IBNS bevezetése

- Monitor Mode – 1. fokozat
  - Csak megfigyelés
    - Eszközök hitelesítési sikerei, MAC címek
  - Elő hitelesítés során minden nyitott
  - Nincs korlátozás az elérhető hálózatban
- Low Impact Mode – 2. fokozat
  - Hozzáférés vezérlés
  - Elő hitelesítés korlátozott hozzáféréssel
  - Hitelesítés után általában minden hozzáférés engedélyezése
  - Nem hoz nagy változtatást a meglévő hálózat konfigurációba
- High Security Mode – 3. fokozat
  - Teljesen zárt elő hitelesítés. A speciális eszközök MAB segítségével hitelesítenek még a 802.X előtt
  - Hitelesítés után a forgalmak elkülönítése VLAN segítségével

NAC készülék (Cisco: Identity Services Engine)

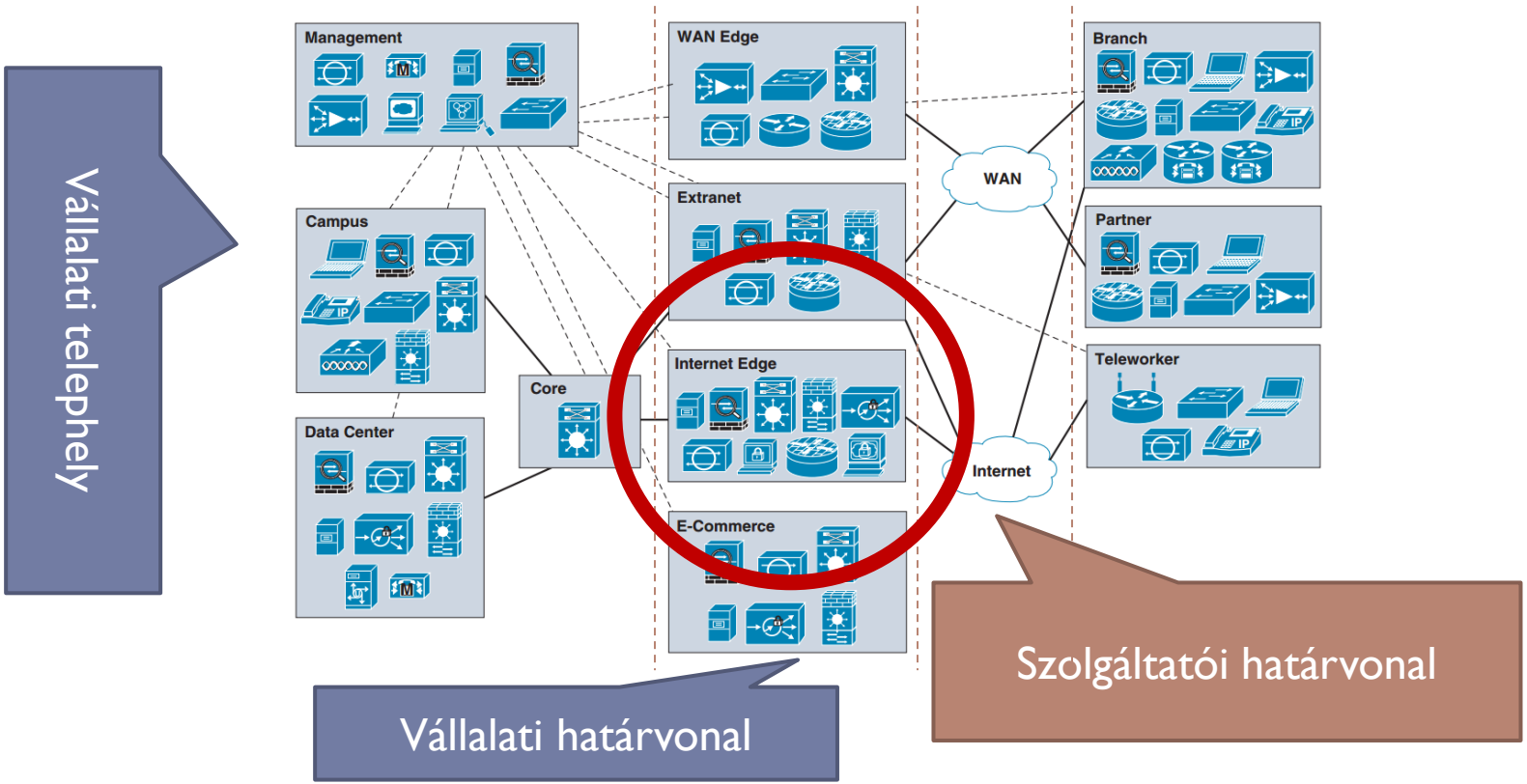
- Biztonságos kliensek
- NAC Manager
  - Házirendek kialakítása
  - Felhasználók menedzselése
  - NAC Server kezelése
- NAC Server
  - Tesztek elvégzése/elvégeztetése
- NAC Agent
  - A felhasználó gépén fut, ellenőrzi a gép biztonságát
    - Patchek, vírusírtó állapota, …
  - Állandó és web alapú kliens
- NAC Profiler
  - A hálózatra csatlakozó eszközök jegyzése
- NAC Guest Server
  - Vendég felhasználók kezelése



Nagyvállalati architektúra

Internet határ

CISCO Enterprise Architecture (CEA)

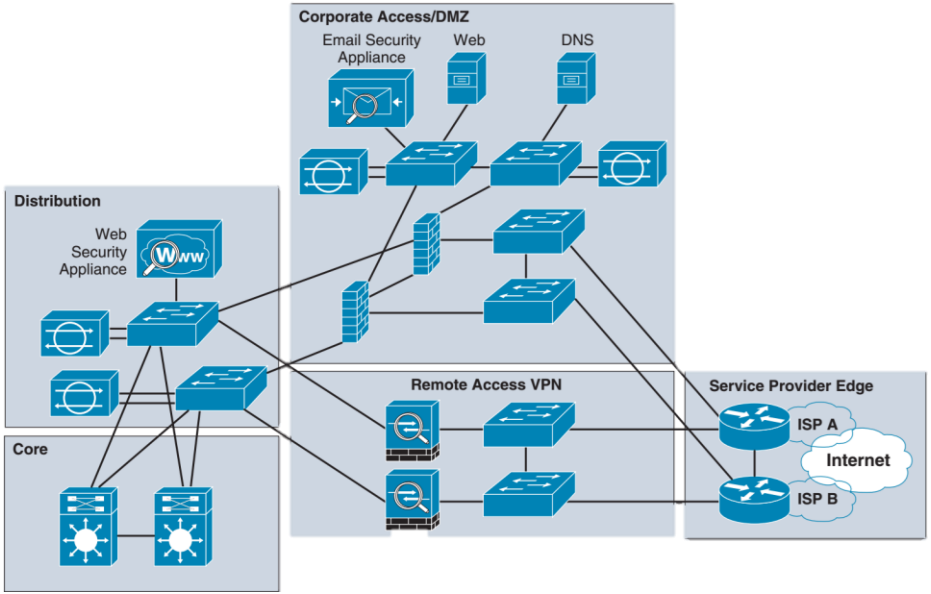


Enterprise Internet Edge

- Kapcsolódás az Internethez
- Gyakran tartalék a WAN eléréshez

- Szolgáltatói határ (SP Edge)
  - Router a szolgáltató felé
  - Redundáns
- Corporate Access/DMZ
  - A vállalat elérése
  - Szolgáltatások az Internet felhasználóknak
    - Demilitarizált övezet
    - WWW, FTP
- Távoli elérés (Remote access)
  - A vállalat elérése távoli dolgozók részére

- Határ elosztási réteg (Edge Distribution)
  - Interfész a nagyvállalati hálózathoz



Fenyegetések

- Interfész a nyilvános hálózat felé
  - Támadások az Internetről
    - DoS és DDoS támadások
    - Alkalmazás, email, webes spyware, malware, adware, virus, spam, phishing
    - Alkalmazási réteg támadások
      - XSS

Védekezések

- Szolgáltatói határ
  - Védekezés redundanciával
    - Több router, több szolgáltató
  - Forgalom optimalizálása, terhelésmegosztás

- Vállalati elérés/DMZ
  - Demilitarizált övezet (DMZ)
    - Minden olyan forgalom, ami nem mehet be a nagyvállalati hálózatba
    - Csak a nyilvánosan elérhető szolgáltatások (WWW, FTP, email, DNS, …)
  - Tűzfalak
    - Kapcsolat megfigyelés (Connection tracking)
    - Deep Packet Inspection (DPI)
    - Web application firewall (WAF)

Védekezések 2.

- Távoli elérés
  - Különböző VPN megoldások
    - SSL VPN: Csak bizonyos HTTP szolgáltatások elérése
  - Hitelesítés, jogosultság kezelés
  - Általában külön tűzfal (nem osztozik a vállalati tűzfallal)

- Határ elosztási réteg
  - Aggregált forgalom, szolgáltatások védelme
  - IDS/IPS megoldások
  - Cisco WSA (Web Security Appliance)
    - Tartalom szűrés
    - URL szűrés, malware és spyware blokkolása
    - Házirendek

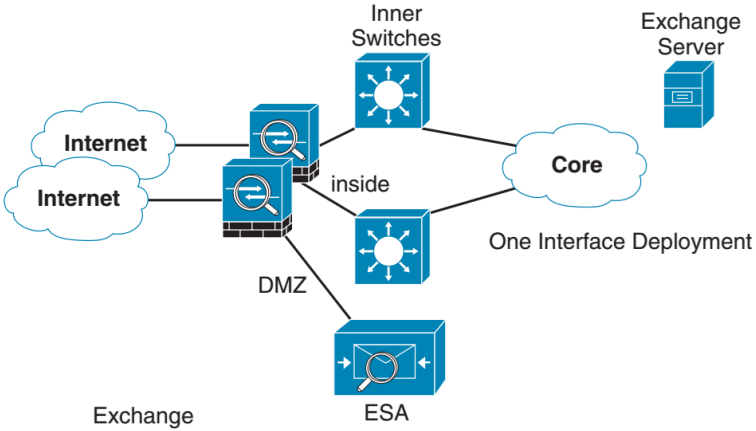
Email és Web biztonság

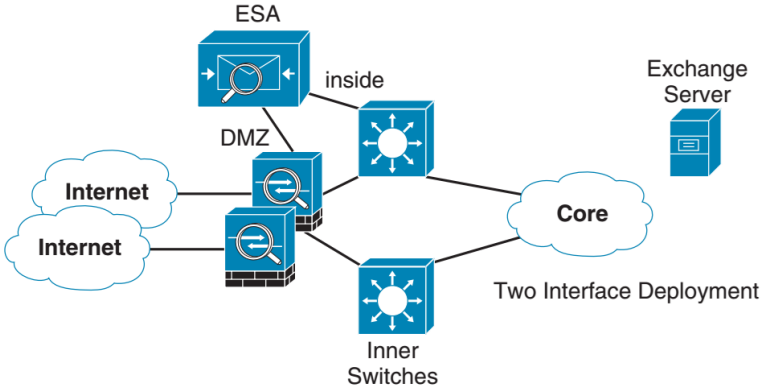
- ESA: Email Security Appliance
- WSA: Web Security Appliance

- Az email és web forgalom figyelése
  - Globális küldési nagyságrendek, spamtrap accountok, DNS feloldás sikere, fekete listák, open-proxy, URL a vírusos levelekben
  - Pontozás különböző faktorok alapján, majd szűrés pontszám alapján (reputation score)

Email és Web biztonság 2.

- Email
  - SMTP (Simple Mail Transfer Protocol)
- Külső és belső emailek elkülönítése
  - Egy interfészes elrendezés
  - Két interfészes elrendezés
- ESA redundancia
  - DNS esetén tartalék MX címek
  - Terhelésmegosztás

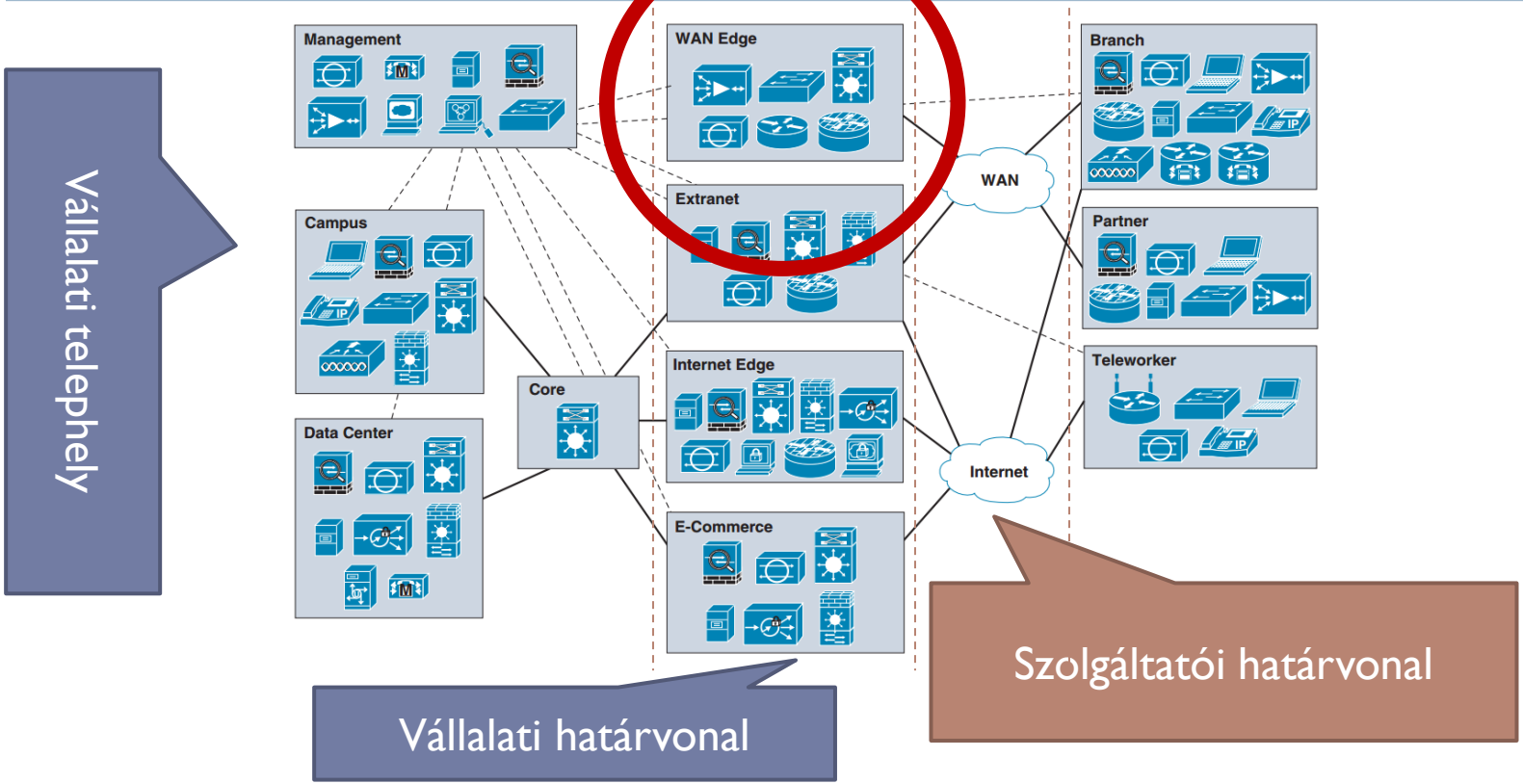




Nagyvállalati architektúra

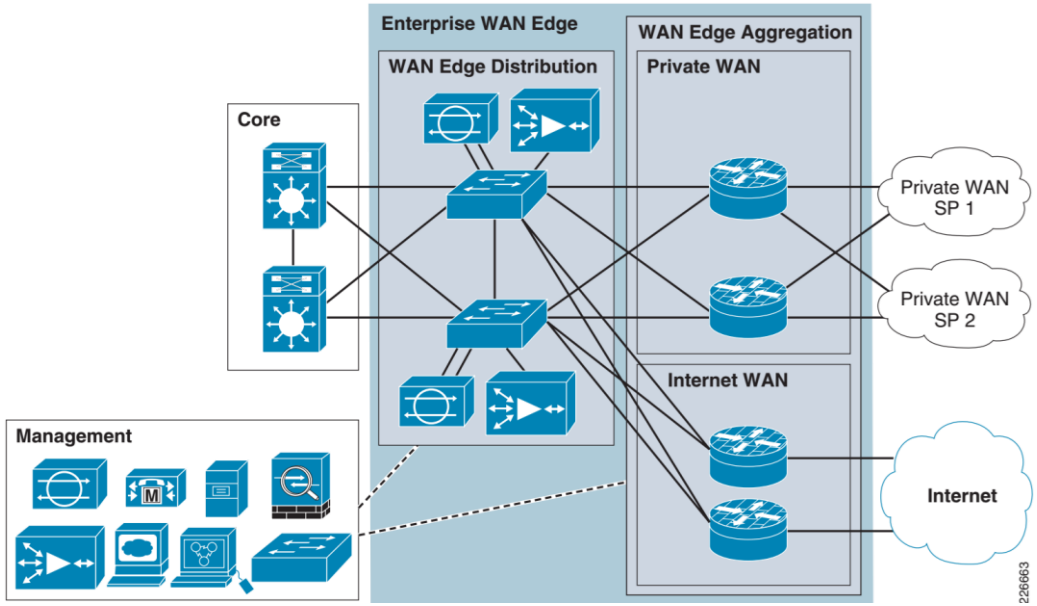
WAN határ

CISCO Enterprise Architecture (CEA)



Enterprise WAN Edge

- Telephelyek összekötése
  - Üzleti alkalmazások
  - Együttműködés
- WAN határ aggregáció
  - Site-to-site VPN
- WAN határ elosztás
  - Hozzáférés a központi réteghez



Fenyegetések

- Telephelyekről induló támadások
  - Trójai, vírus, botnet
- WAN hálózatban támadások, közbeékelődéses támadás (MITM)
- Jogosulatlan hozzáférés, jogosultság emelés
- DoS

Védekezés

- WAN kapcsolat védelme
  - WAN forgalom elkülönítése
    - Hitelesítés, integritás védelem
    - VPN segítségével, MPLS segítségével
    - IPSec
  - WAN hozzáférés hitelesítése
    - Erős hitelesítés
      - PKI alapon
  - WAN forgalom titkosítása
    - Erős titkosítás (pl.: AES)

WAN határ elosztási réteg

- IPS/IDS megoldások
  - Inline vagy promiscuous mód
  - Skálázhatóság
  - Kétirányú forgalom figyelése!
    - Másolás, egyetlen kapcsoló, forgalomirányítás, ‘sticky’ terhelésmegosztás
- Forgalomirányítás biztonsága
  - Szomszédok hitelesítése
  - Naplózás