Předmět:	**Projektování IS I**
Téma:	**Architektury pro bezpečnost a spolehlivost IS/IT**

Vyučující:	dr. Dušan Kajzar	Školní rok:	2020/2021

Obsah:

1. Úvodem k architekturám BIS a HA

Zaměření této přednášky:

- zaměříme se na architektonická schémata podporující bezpečnost, spolehlivost a vysokou dostupnost IS,
- tzv. architektonické návrhové vzory.

Architektury podporující BIS a HA:

- BIS – bezpečnost inf. systémů,
- HA – High Availability (vysoká dostupnost).

Architektonické návrhové vzory IS/IT:

- schémata často se vyskytující při návrhu podnikových IS,
- dané schéma (návrhový vzor)
  - zaměřené na splnění požadovaných vlastností navrhovaného IS,
  - např. spolehlivost, dostupnost, bezpečnost, ...

2. Architektury pro bezpečnost a spolehlivost IS

Bezpečnost systému:

- schopnost systému zajistit požadovanou - integritu, důvěrnost, dostupnost IS,
- integrita dat – neporušitelnost dat,
- důvěrnost dat – přístup k datům pouze oprávněným uživatelům,
- dostupnost IS – viz dále.

Dostupnost (availability) systému:

- vysoká dostupnost – HA, High Availability,
- schopnost být uživateli (podnikovému procesu) k dispozici,
- v souladu se stanovenými parametry dostupnosti služeb
  - např. dostupnost služby ve dnech ..., v době od-do, ...
  - např. 5*12, 7*24, po-pá 6-18, ...
  - nebo (resp. navíc) procentuálně ... 98.5, 99.8, ...
- v souladu se stanovenými parametry výkonnosti
  - s dobou doba odezvy= ... ,
  - max. čas pro zpracování požadavku = ...
- v mezích akceptovatelnosti případných výpadků
  - max. provozně akceptovatelná doba výpadku,
  - v provozní špičce = ..., mimo špičku = ... ,
- s garancí časů pro obnovu dat / služeb IS po výpadku
  - recoverytime – max. čas, za který je bezpodmínečně nutno obnovit služby systému,
  - recovery point – max. provozně tolerovatelná ztráta práce po havárii.

Spolehlivost (reliability) systému:

- schopnost systému poskytovat služby
  - podle stanovených parametrů dostupnosti,
  - podle stanovených parametrů bezpečnosti,
- spolehlivý systém nesmí selhat v oblasti dostupnosti ani bezpečnosti,
- v praxi – stupeň spolehlivosti se sleduje, měří a vyhodnocuje
  - počty a doba výpadků, procentuální dostupnost, ...

    - bezpečnotní incidenty a jejich příčiny, ...
- => návrhy na organizační a technická opatření, vylepšení,
- srovnej – spolehlivost auta, pračky, mobilu, ...

Spolehlivost IS závisí:

- na spolehlivosti jeho jednotlivých komponent (HW, SW)
    - je ovlivněna „nejslabším článkem“ IS (!),
    - závisí na kvalitě IS jako celku,
- na kvalifikaci uživatelů IS (proškolení, znalosti práce s IS),
- na kvalitní správě podnikových IS (administrátoři IS, support).

Mnohá selhání IS:

- mají lidské nebo organizační příčiny (IS je sociotechnický systém),
- lepší metody a IT - nemusí automaticky zajistit lepší spolehlivost a bezpečnost (např. moderní automobil, ale špatný řidič).

Základní technické principy pro zajištění spolehlivosti IS:

- redundance (nadbytečnost) komponent,
- diverzifikace (rozmanitost) komponent.

Princip redundance:

- systém má rezervní (sekundární) součásti, které lze použít v případě selhání některé primární součásti,
- redundance „součástek“ - např. síťových karet, řadičů diskového pole, ...
- redundance subsystémů (komponent) - např. aplikačních serverů, firewallů, diskových polí, ...

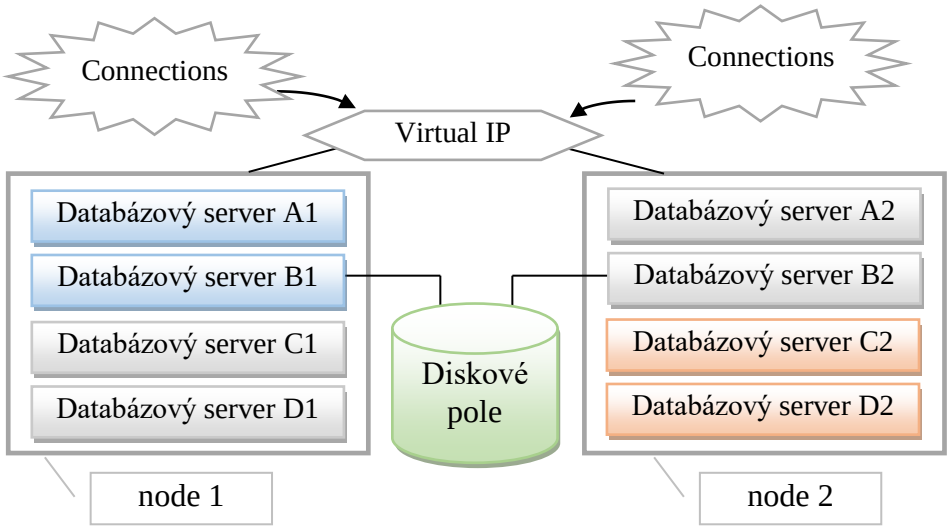
Princip diverzifikace (rozmanitosti):

- redundantní součástí jsou různého typu (snížení pravděpodobnosti, že neselžou stejným způsobem),
- rozmanitost v lokalizaci výpočetní techniky (různé serverovny, různé lokality).

3. Clusterová řešení

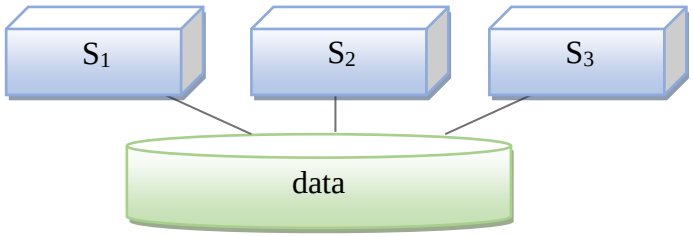
Schéma a princip clusterového řešení:

- systémy (služby) pracující nad společným datovým prostorem,
- datový prostor je zviditelněný z „jedné či druhé“ strany,
- Active / Passive (Standby),
- Active / Active.



Ve vývojové praxi to pro architekta znamená:

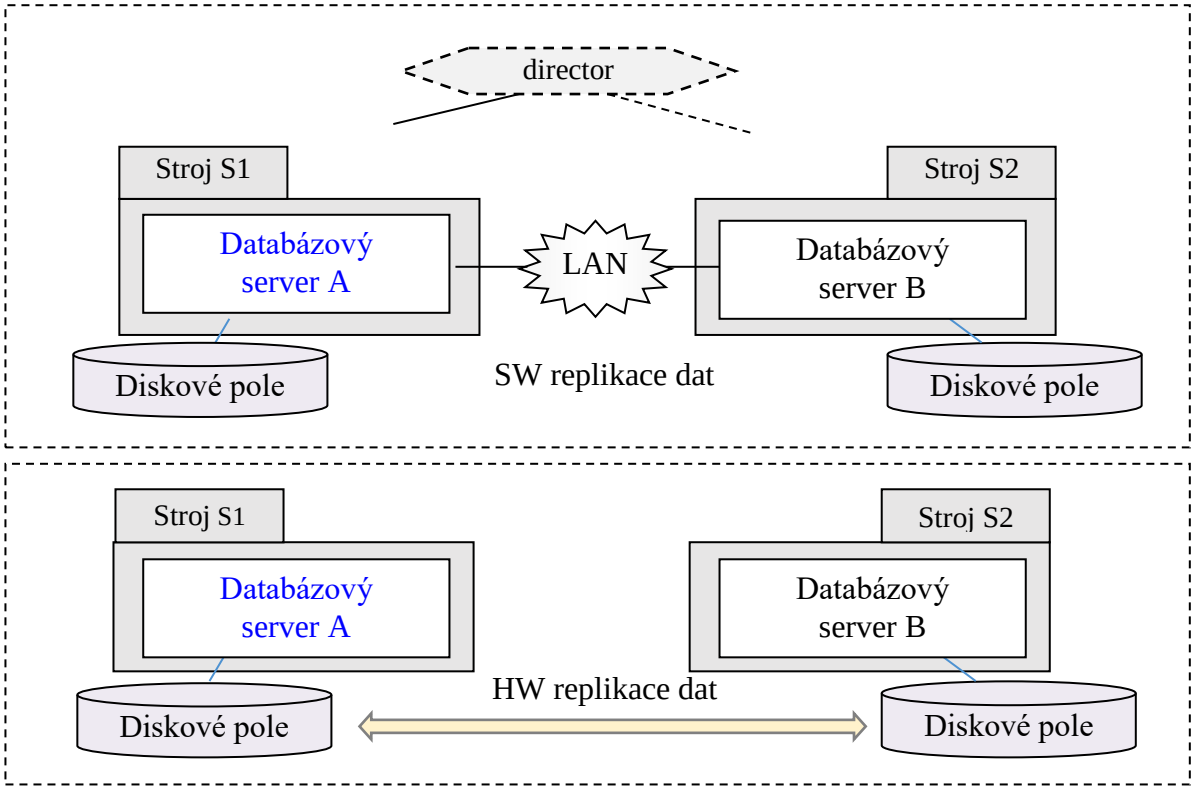
- zvolit režim běhu SW komponent
  - Active/Active, Active/Passive,



- pro režim A/P
  - navrhnout pravidla běhu a migrací SW komponent (služeb),
  - tj. na kterém nódu daná SW komponenta poběží primárně,
  - který nód bude pro SW komponentu záložní (je-li nódů v clusteru více),
  - zvážit zdroje (CPU, paměť) pro provoz na záložním nódu,
  - způsob migrace na záložní nód – automaticky, ručně,
  - atd.

Standby systémy:

- relativně samostatné systémy s vlastními datovými prostory,
- režimy Hot standby, Warm standby , Cold standby.



K režimům Standby - Hot, Warm, Cold:

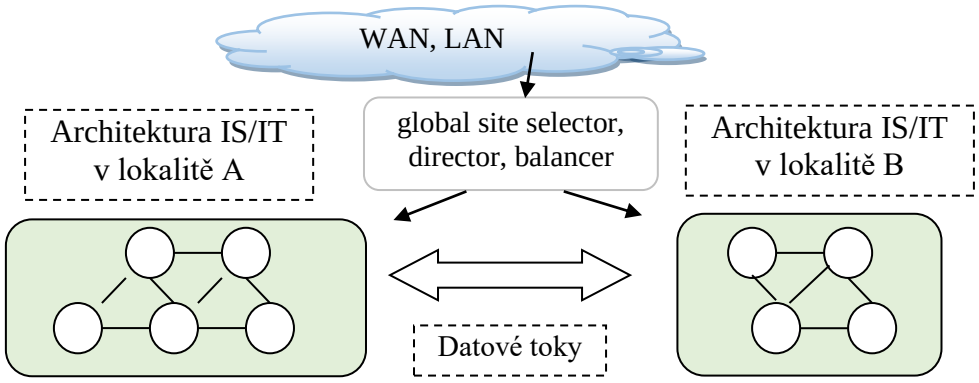
- Hot Standby
  - synchronní HW replikace (na úrovni diskových polí),
  - DB - dvoufázový commit (synchronní přenos dat),
- Warm Standby
  - SW replikační mechanismus (asynchronní přenos dat),
  - asynchronní HW replikace (na úrovni diskových polí),
- Cold Standby
  - předinstalovaný (částečně, úplně) server, vypnutý.

Příklady DB technologií Warm Standby:

- MS SQL Server Mirroring (db hlavní, zrcadlená, witness),
- Sybase Standby DB,
- Oracle Data Guard.

Geocluster:

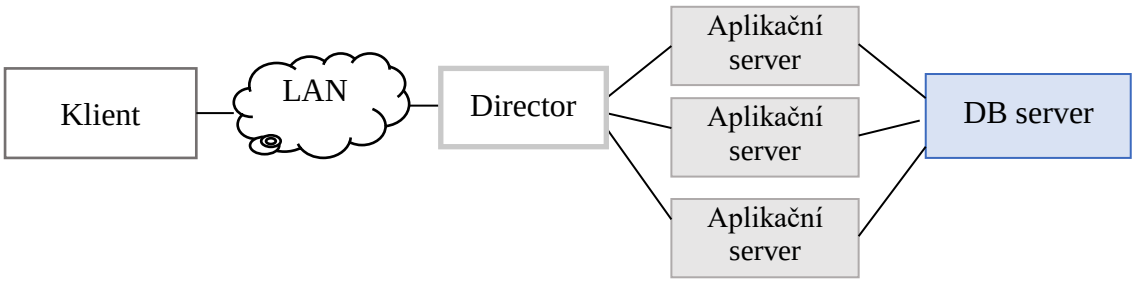
- architektura pro více výpočetních center,
- v clusteru nejsou jen jednotlivé systémy (AS, DB, ...), nýbrž celá výpočetní centra,
- režim Active / Passive, režim Active / Active.

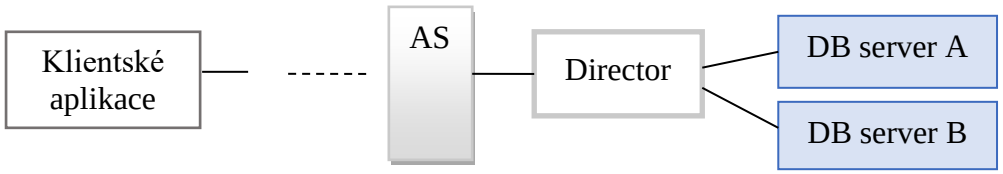


4. Architektury síťové vrstvy

Balancing nad APL/DB servery:

- se zvýšenou odolností proti výpadku komponenty
  - tzv. režim failover,
- s vyrovnáváním zátěže mezi servery
  - tzv. režim load-balancing.





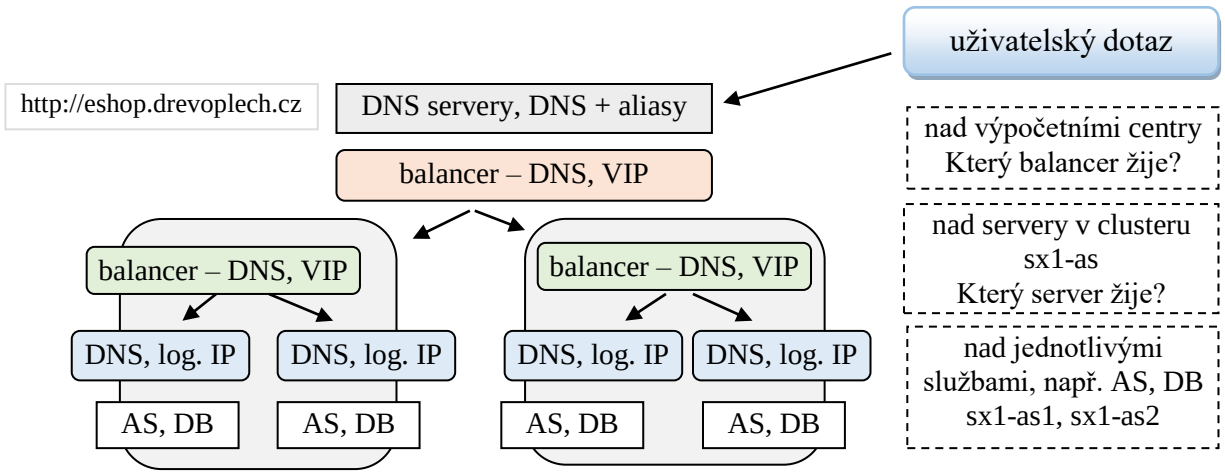
Význam a využití directorů (balancerů):

- HW a SW komponenty sloužící k řízení spojení
  - tzv. sessions, connections,
  - tj. spojení, která směřují k AS nebo DB serverům,
- směrování dotazů podle daných směrovacích pravidel
  - na základě cíle (URL),
  - podle typů (skupin) uživatelů (interní, externí, public, registrovaní, ...),
  - podle vlastností SQL dotazu, kategorie složitosti dotazu, ...
- režimy práce balanceru
  - load balancing,
  - fail-over,
- mohou zahrnovat i pravidla pro ochranu před zahlcením systému dotazy
  - základní rozhodovací algoritmus (kam směrovat dotaz) - roud robin,
  - rozhodování podle zatížení jednotlivých komponent,
  - podle počtu connections vedoucích na jednotlivé komponenty, ...
  - zajištění tzv. „držení sešny“ na daném aplikačním serveru.

Příklady directorů a balancerů:

- Cisco ACE modul,
- Big-IP F5,
- Teradata Unity Director.

Směrování a balancing v architekturách síťové vrstvy:

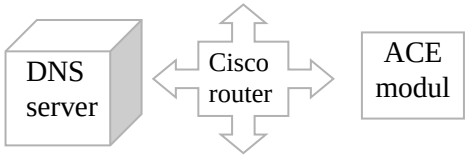


Dotazy:

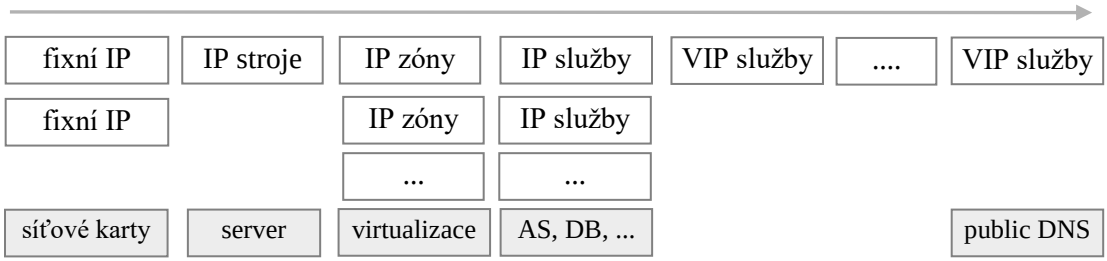
- Nad jakými komponentami balancují znázorněné balancery?
- Na kterou VIP odkazuje DNS služby, kterou volá uživatelova aplikace?

Virtuální IP:

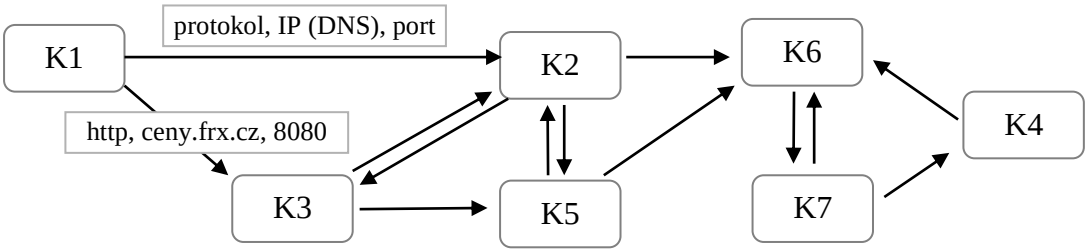
DNS	VIP
http://eshop.firma.cz	10.128.251.35
https://products.firma.cz	certifikát



Hierarchie IP adres:



Návrh vzájemné komunikace komponent IS:



Zadání komunikace mezi komponentami IS:

- co není výslovně povoleno, to je zakázáno (!),
- definice komunikace (filtrace spojení) do tzv. Access listu
  - správce sítě -> nastavení na síťových prvcích,
- zdroj (odkud): IP + cíl (kam): IP, port,
- komunikace jednosměrná, obousměrná.

Důležité téma - síťová bezpečnost:

- šifrování přenosů dat,
- demilitarizovaná zóna, detektory útoků, ...

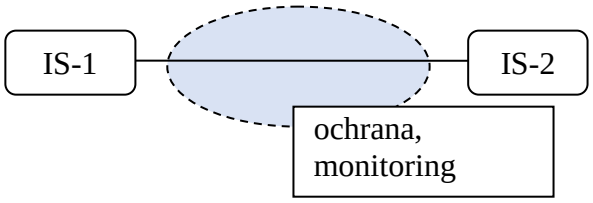
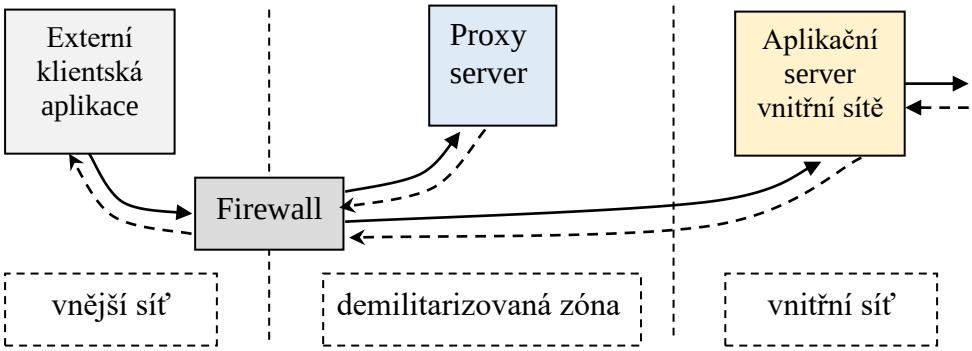
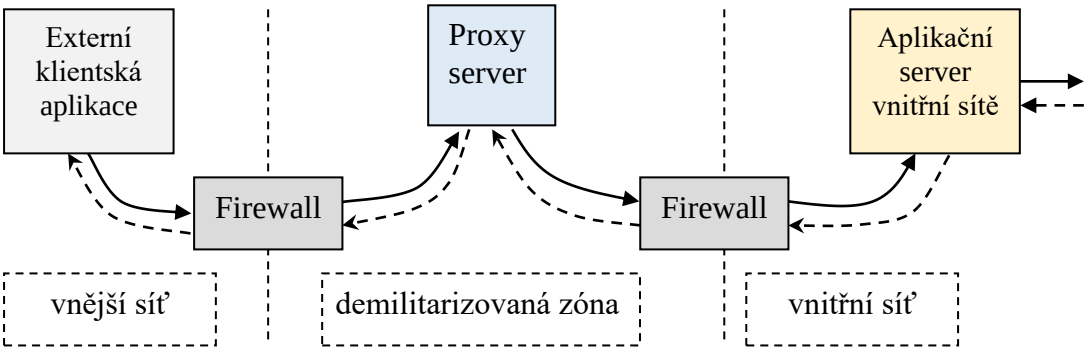


Schéma demilitarizované zóny počítačové sítě:

- DMZ – počítačová podsíť tvořící bezpečnostní vrstvu mezi interní podnikovou sítí a Internetem,
- DMZ s jedním firewallem (trojnohý FW)
  - 3 síťová rozhraní,
  - komunikace – Internet, DMZ, vnitřní síť.



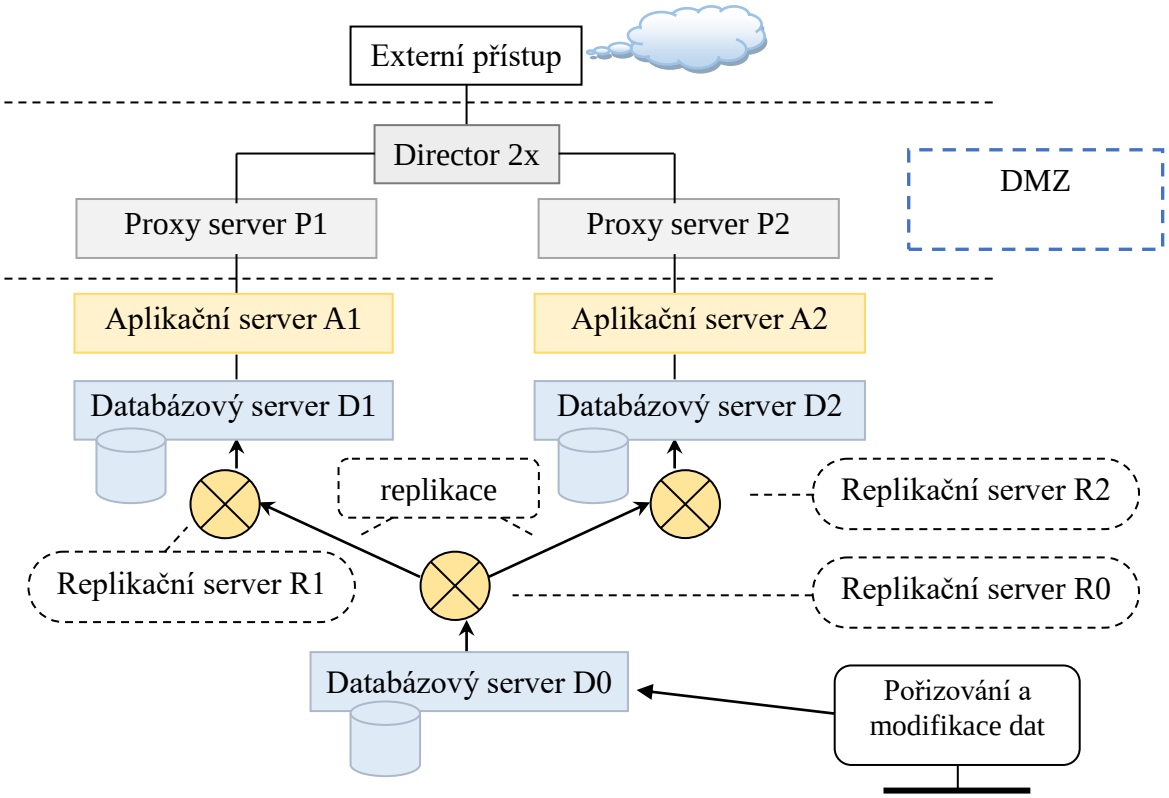
- DMZ se dvěma firewally (dvojnohý FW)
  - frond-end firewall – kontrola komunikace Internet x DMZ,
  - back-end firewall – kontrola komunikace DMZ x vnitřní síť.



V praxi nutno řešit např.:

- povolená / nepovolená komunikace mezi DMZ a vnitřní síti (IP, porty, protokoly),
- které komponenty IS budou umístěné do DMZ,
- způsob zálohování serverů umístěných v DMZ, ...

„V-architektura“ webové aplikace:



5. Dokumentace k architekturám podnikových IS

Dokumentace k architektuře aplikace (IS) obvykle popisuje:

- účel daného IS v podniku,
- stanovené parametry (kategorie) dostupnosti a bezpečnosti,
- kdo je gestorem daného IS, dodavatelem, support, ...
- hlavní subsystémy daného IS a jejích vazby na okolí,
- přístupy k IS ze strany klientů (URL),
- integraci IT služeb - poskytování služeb jiným IS a opačně,
- HW a SW architekturu
  - prezentační vrstvy,
  - aplikační vrstvy,

    - databázové vrstvy,
- architekturu vazeb IS na společné síťové úložiště NAS,
- architekturu datových toků (replikace dat)
    - v rámci komponent IS + vazby s okolím,
- architekturu sítových prvků vztahujících se k danému IS
    - DNS, VIP, IP adresy, balancery, ...
- architekturu síťových komunikačních toků
    - v rámci komponent IS + vazby s okolím,
    - komunikační protokoly,
    - IP, porty, komunikace odkud-kam,
- architekturu licenčního pokrytí komponent.