Antispam Gateway

–

pračka elektronické pošty

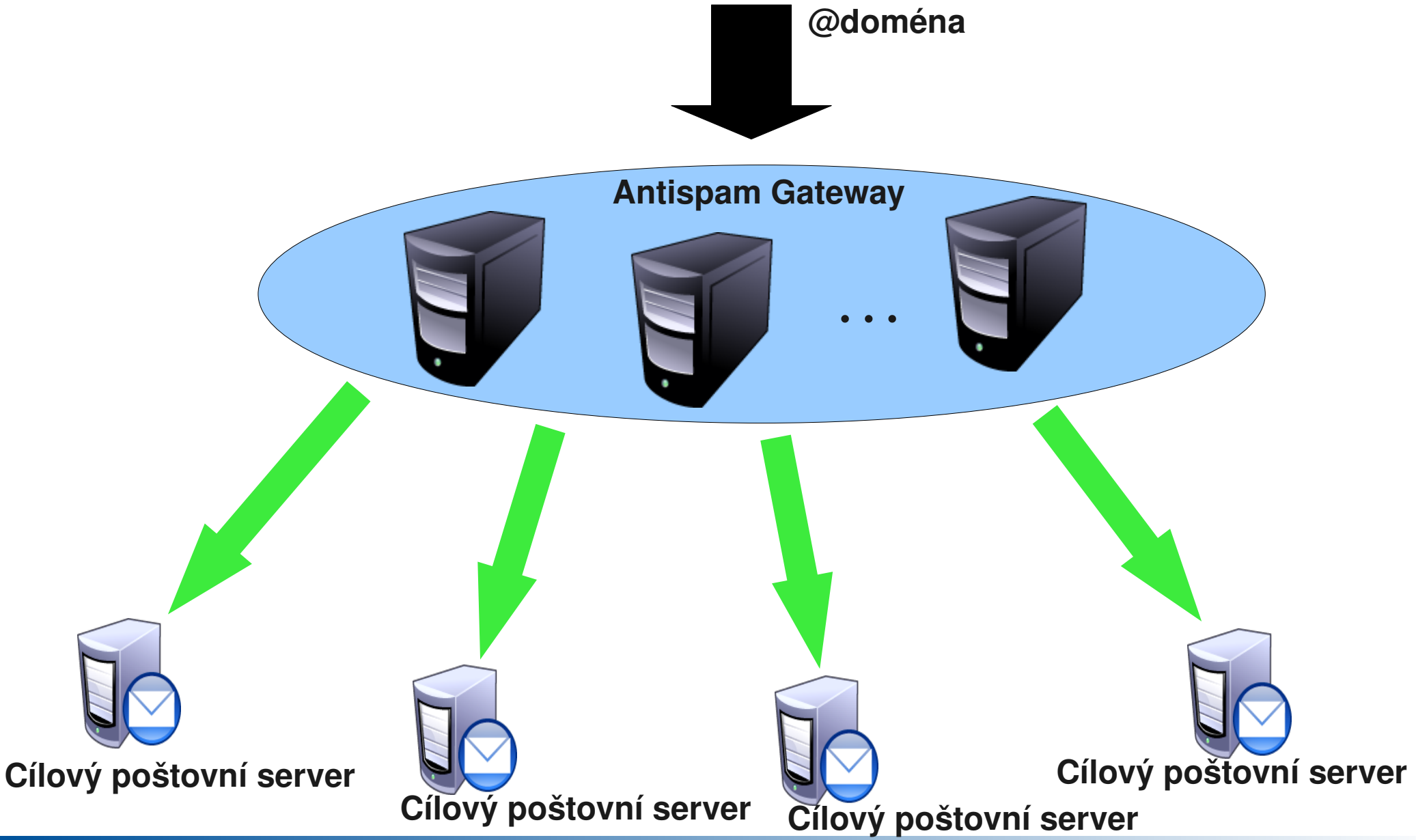
Andrea Kropáčová, andrea@cesnet.cz
CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

Antispam Gateway

- **Služba zajišťuje**
  - nepřijetí (odmítnutí) nevyžádané pošty
  - antivirovou a antispamovou analýzu zpráv
  - doručení ohodnocených zpráv na koncový poštovní server
- **Impuls pro zřízení služby**
  - je to oblast, kterou umíme opravdu dobře
  - správa a-a ochrany je finančně i personálně náročná
  - řešení „na klíč“ prostřednictvím třetích stran jsou drahá
  - čím větší provoz, tím je ochrana účinnější

Jak služba funguje



Jak služba funguje

- Služba je poskytována **doméně** (cesnet.cz)
- **MX záznam** domény je **nasměrován na AG**
- **Proces zpracování příchozích zpráv na AG**
  - část zpráv je odmítnuto na vstupu („nepřijato“)
  - je provedena analýza zprávy (spam, vir)
  - výsledek analýzy je vložen do hlavičky zprávy
  - zpráva je zaslána na cílový poštovní server

```
X-spam-status:
X-spam-level:
X-spam-virus:
X-spam-report:
X-spam-greylist:
```

- **Zpracování zpráv na cílovém poštovním serveru**
  - „zahodit“
  - zařadit do složky speciálně k tomu určené (spam)
  - zařadit mezi příchozí zprávy (ham)
  - *teoreticky je možná další analýza*

Hlavní výhody služby

- Robustní architektura, **vysoká účinnost ochrany**;
- **Není třeba provozovat** (platit, vyvíjet, udržovat) **vlastní a-a systém**, odpadá starost o správu HW, SW a licence;
- Umožňuje **zpracování výsledku analýzy zpráv až na cílovém poštovním serveru**;
- Funguje zároveň jako **záloha poštovního provozu**;
- Zaručujeme **korektní zacházení se zprávami**;
- **Minimální zásah** do vnitřní infrastruktury cílového poštovního serveru;
- **Nezávislost na** typu cílového poštovního serveru;
- Modularita a-a ochrany – **možnost integrace i komerčních řešení.**

Technická realizace služby

- **Probíhá v těchto krocích**

1) Diskuse o potřebách instituce (domény)
2) Příprava cílového poštovního serveru
    - nastavení propojení cílového serveru s AG
    - nastavení cílového serveru
3) Testovací fáze
    - test komunikace AG a cílového serveru
    - test připravenosti cílového příjemce
4) Nastavení MX záznamů domény (směr na AG)
5) Zvýšené monitorování provozu
6) Úprava systému AG “na míru”

Provoz služby

- AG je monitorována
  - dohled zajišťuje Pracoviště Stálé Služby (24/7/365), + 420 2 2435 2994
- Je prováděna systematická kontrola provozu
  - výskyt chybových stavů
  - místa pro zlepšení funkcionality
  - statistika provozu služby pro doménu
- Uchování provozních údajů
  - možnost dohledat “co se děje”, “co se stalo“ ...
  - možnost dohledat kdy a kam byl mail směrován a doručen
- Funkce ***záložní poštovní server***
  - „on demand“ možnost prodloužení doby pozdržení zpráv
  - možnost přesměrování na jiný cílový server

Antispam Gateway

- **Služba je vhodná pro**
  - menší instituce
  - menší sítě/domény
  - sítě/domény s malým až středním provozem
- **Služba není otestována pro instituce (domény)**
  - s velkým objemem pošty
  - hierarchickou architekturou poštovních služeb
  - s velkou četností změn ve směrovacích pravidlech
  - ???

Děkuji za pozornost.