

# Zabezpečený přístup do intranetu

Bakalářská práce, FEL ČVUT Praha

Michal Turek

Vedoucí práce: Doc. Ing. Zdeněk Kouba, CSc.

červenec 2007

1. Seznamte se s problematikou bezpečného zpřístupnění legacy databáze z Internetu za následujících omezujících podmínek:
  - 1.1 Databáze je provozována na serveru, jehož adresa je překládána (NAT), tudíž není viditelná z Internetu
  - 1.2 Bezpečnostní politika neumožňuje port tunneling pro porty používané databázovým serverem
  - 1.3 Schéma databáze není možné pro účely zpřístupnění z Internetu měnit
2. Na základě analýzy problému z bodu 1. navrhnete middleware umožňující požadovaný přístup z Internetu.
3. Navržený systém implementujte a vyhodnoťte, jaký je nárůst režie zpracování ve srovnání s přístupem zevnitř intranetu

Zadání práce

Návrh

Analýza

NAT

Odstínění RMI

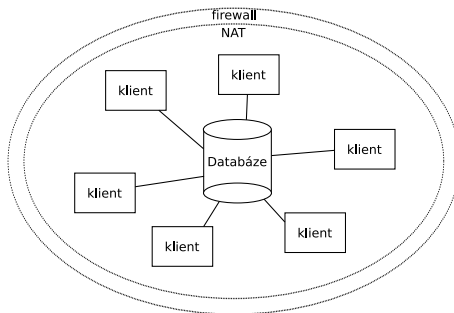
Režie řešení

Shrnutí

# Původní architektura systému

Zabezpečený  
přístup do  
intranetu

Michal Turek



- Databáze: PostgreSQL
- Klienti: Grafické aplikace napsané v jazyce Java
- **Databáze kvůli bezpečnosti nepřístupná z Internetu**

Zadání práce

Návrh

Analýza

NAT

Odstínění RMI

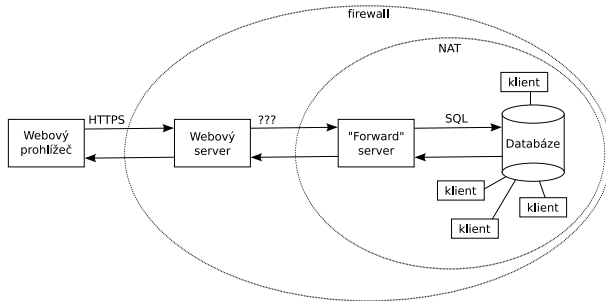
Režie řešení

Shrnutí

# Předběžný návrh nové architektury systému

Zabezpečený  
přístup do  
intranetu

Michal Turek



Zadání práce

Návrh

Analýza

NAT

Odstínění RMI

Režie řešení

Shrnutí

- ▶ Původní systém zůstane kompletně zachován
- ▶ Webový server nekomunikuje s databází přímo
- ▶ **Návrh a implementace forward serveru**
- ▶ Zprovoznění celého komunikačního řetězce

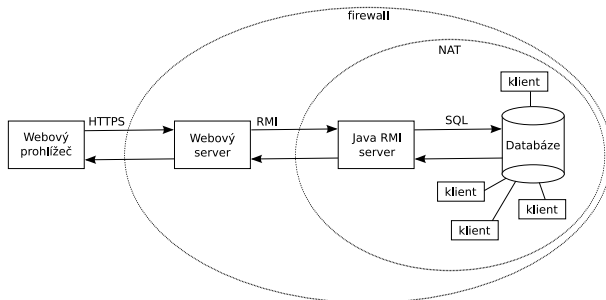
- ▶ Jazyk PHP
- ▶ **Java servlety a JSP**
- ▶ Java applety
- ▶ CGI skripty
- ▶ ASP.NET
- ▶ ...

- ▶ Řešení na bázi vzdáleného volání funkcí
- ▶ Remote Procedure Call (RPC)
- ▶ Protokoly založené na XML
  - ▶ XML-RPC
  - ▶ SOAP
  - ▶ ...
- ▶ Binární komunikační protokoly
  - ▶ Corba
  - ▶ **Java RMI**
  - ▶ ...

# Navrhovaná architektura systému

Zabezpečený  
přístup do  
intranetu

Michal Turek



- Webový server: Java servlety a JSP
- Forward server: Java RMI server
- Komunikační protokol: Java RMI

Zadání práce

Návrh

Analýza

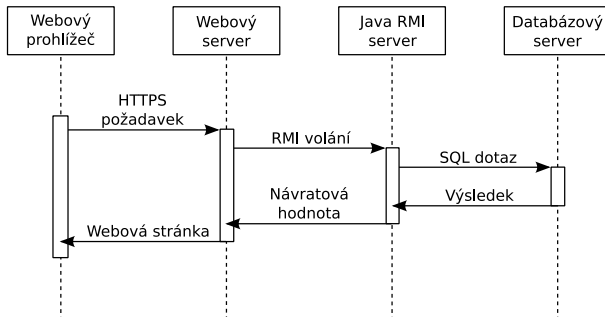
NAT

Odstínění RMI

Režie řešení

Shrnutí

# Sequence diagram přístupu k databázi



Zadání práce

Návrh

**Analýza**

NAT

Odstínění RMI

Režie řešení

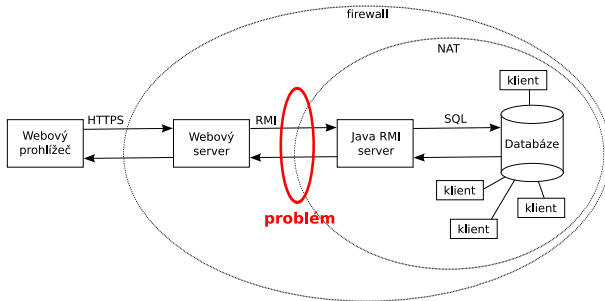
Shrnutí



# Komunikace přes NAT

Zabezpečený  
přístup do  
intranetu

Michal Turek



- ▶ Webový server nevidí forward server
- ▶ Webový server otevírá spojení
- ▶ **Přeposílání paketů NATem?**
- ▶ Jiné řešení?

Zadání práce

Návrh

Analýza

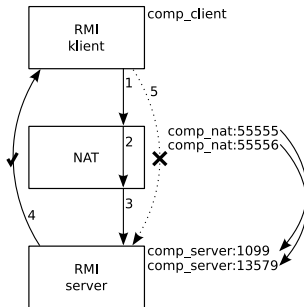
**NAT**

Odstínění RMI

Režie řešení

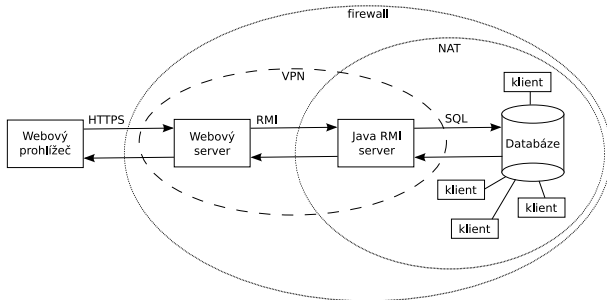
Shrnutí

# Problém s komunikací přes NAT



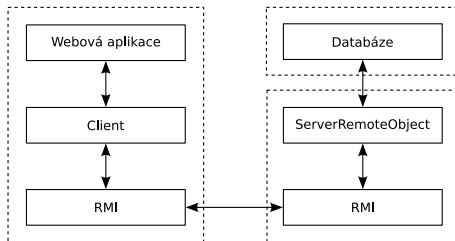
1. Klient pošle data na comp\_nat:55555
2. NAT je přepoše na comp\_server:1099
3. Data bez problémů dojdou
4. **Rmiregistry: vzd. objekt je na comp\_server:13579**
5. Klient se pokouší připojit přímo - chyba

# Dvě řešení problému s NATem



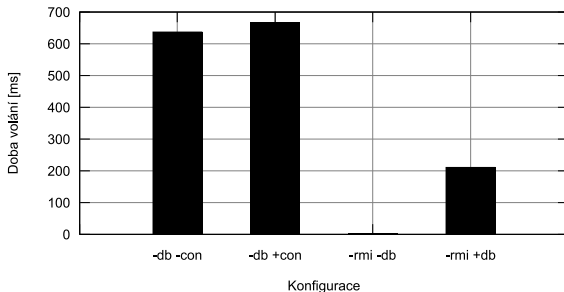
- ▶ VPN mezi webovým a RMI serverem
- ▶ Programové řešení v Javě
- ▶ Obě řešení víceméně ekvivalentní
- ▶ **Obě úspěšně zprovozněna a použitelná**

# Komunikace mezi jednotlivými částmi aplikace s použitím třídy Client



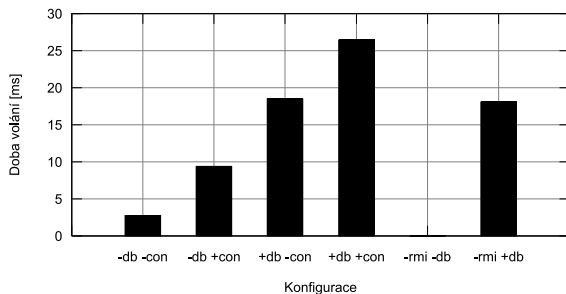
- ▶ Třída Client přidává další mezivrstvu
- ▶ **Umožňuje velice jednoduše odstínit RMI**
- ▶ Přímý přístup webového serveru k databázi
- ▶ Parametr `use_rmi` v konfiguračním souboru

# Graf doby prvního volání vzdálené metody

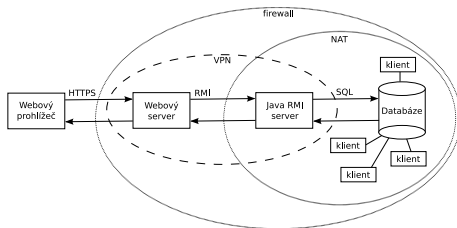


- ▶ db - vzdálená metoda přistupuje k databázi
- ▶ con - po každém volání se zruší spojení s RMI serverem
- ▶ rmi - k databázi se přistupuje nepřímě přes RMI server (implicitní)

# Graf doby následujících volání vzdálené metody



- ▶ db - vzdálená metoda přistupuje k databázi
- ▶ con - po každém volání se zruší spojení s RMI serverem
- ▶ rmi - k databázi se přistupuje nepřímě přes RMI server (implicitní)



- Implementováno obecné, snadno rozšiřitelné řešení
- Možnost odstínění RMI, přímá komunikace s databází
- Použité technologie: Java servlety a JSP, Java RMI
- Webový server: Apache Tomcat
- Databázový server: PostgreSQL, MySQL
- Operační systém: Debian Etch GNU/Linux, FreeBSD

Zadání práce

Návrh

Analýza

NAT

Odstínění RMI

Režie řešení

Shrnutí

# Konec prezentace

Zabezpečený  
přístup do  
intranetu

Michal Turek

Zadání práce

Návrh

Analýza

NAT

Odstínění RMI

Režie řešení

**Shrnutí**

- ▶ Otázky?
- ▶ **Děkuji za pozornost**