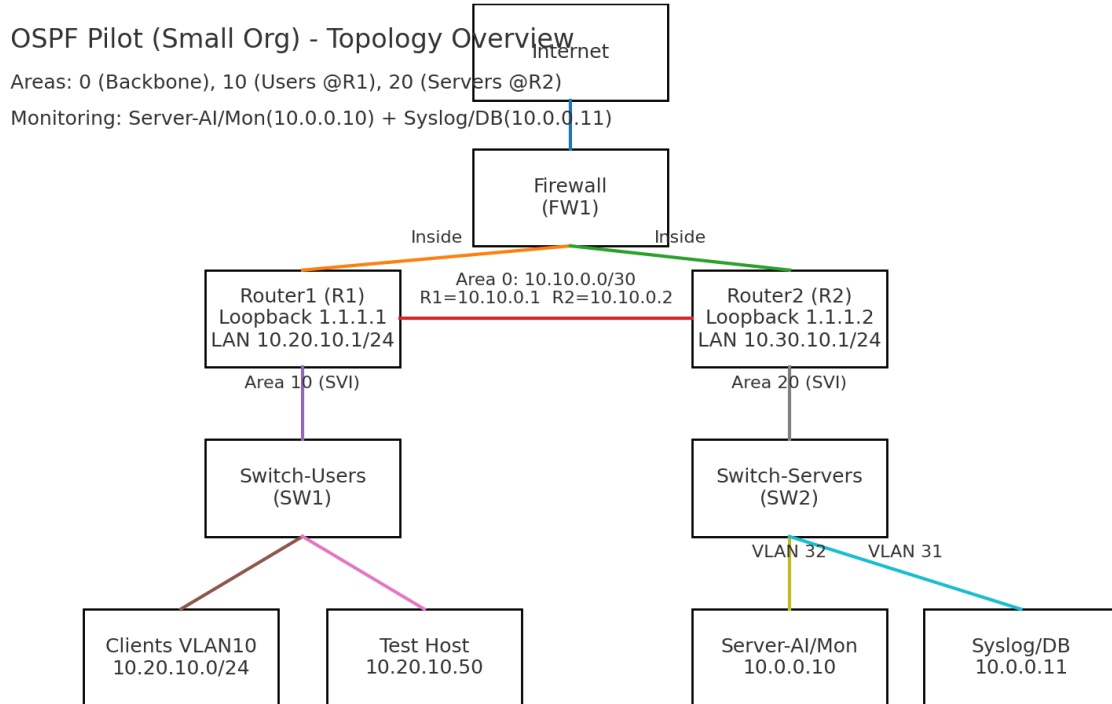


# Pilot



1) چندتا چی لازم داریم و کجا بگذاریم؟

- ۱ دیتاسنتر کوچک (یا یک اتاق سرور)

- ۱ فایروال (FW1) بین اینترنت و شبکه داخلی
- ۲ روتر لایه ۳ (R1 و R2) برای تست OSPF و چند ناحیه
- ۲ سوئیچ لایه ۲: SW1 (کاربران) و SW2 (سرورها/مدیریت)
- ۲ سرور مجازی

◦ Server-AI/Mon (Zabbix/Prometheus + Python Rule Engine)

◦ Syslog/DB (rsyslog + PostgreSQL)

• ۵-۱۰ کلاینت تست (اختیاری)

چیدمان: اینترنت → FW1 → (داخل) R1 و R2. زیر R1 VLAN  
کاربران، زیر R2 VLAN سرورها/مدیریت. مانیتورینگ و پایگاه داده پشت  
SW2

## OSPF Areas

- Area 0 (Backbone): R1 ↔ R2 + Loopback لینک
- Area 10 (Users): R1 زیر VLAN کاربران
- Area 20 (Servers): R2 زیر VLAN سرورها/مدیریت

مزیت: با سه ناحیه می‌توان قوانین «LSDB desync»، «Area mismatch» و «Timer mismatch» را واقعا تست کرد

## IP-Plan (3)

- Backbone R1↔R2 (Area 0 P2P): 10.10.0.0/30 → R1=10.10.0.1, R2=10.10.0.2
- Loopbackها: R1=1.1.1.1/32, R2=1.1.1.2/32 (Area 0)
- Users VLAN (Area 10): 10.20.10.0/24 → SVI R1=10.20.10.1
- Servers VLAN (Area 20): 10.30.10.0/24 → SVI R2=10.30.10.1
- Management/Monitoring: 10.0.0.0/24 → Server-AI/ Mon=10.0.0.10, Syslog/DB=10.0.0.11
- Default route: OSPF به اینترنت؛ داخل شبکه FW1 روی

## Rule-Engine (برای مانیتورینگ و جمع‌آوری داده‌ها)

- Zabbix/Prometheus برای 10.0.0.10 روی ICMP/SNMP/SSH polling
- Syslog logging host 10.0.0.11 روی 10.0.0.11؛ روی روترها

- Poller (SSH با Netmiko/NAPALM) هر 2-5 ثانیه:
- show ip ospf neighbor → state, dead timer remaining
- show ip ospf database → و محاسبه LSA های header استخراج  
lsdb\_hash
- show ip route ospf, show ip ospf → hello/dead/area
- 
- (DB/CSV) ساختار رکورد:  
ts, router\_id, intf, area, neighbor\_id, state, hello,  
dead, lsdb\_hash, lsa\_count, spf\_runs, cpu, mem,  
syslog\_recent

## (6) قواعد Rule-Based (حداقلی لازم برای پروپوزال)

1. Area mismatch: اگر  $\text{area(intf)} = \text{ideal\_area} \rightarrow \text{High}$
2. Timer mismatch: اگر hello/dead با همسایه برابر نیست و  $< 2$   
اسنپشات تکرار شد  $\text{Medium} \rightarrow \text{High}$
3. LSDB desync: اگر  $R1 \neq R2$  lsdb\_hash به مدت  $< 10s \rightarrow \text{High}$   
(+ ذخیره DB کامل)
4. Adjacency flapping: اگر تغییر  $\text{state} > 3$  بار در ۱ دقیقه  $\rightarrow \text{High}$

5. Auth failure (اختیاری): syslog شامل کلید/پیام MD5/Key chain → Critical

## 7) تزریق خطا برای آزمایش

- Mismatch Area: روی R1 یا R2 یک اینترفیس را از Area 0 به Area 10/20 تغییر بده.
- Timer mismatch: فقط یک سمت hello/dead را تغییر بده.
- LSA churn/desync: یک سمت P2P را short flap کن یا یک SVI را up/down کن.
- Adjacency flap: shutdown/no shut چندباره لینک
-