

WORKSHOP GARR 2025

NET MAKERS

Semplificazione e Sicurezza: nuova architettura di Firewall e Routing

Giancarlo Galluzzi, Luca Giuliani
Università degli Studi di Milano

Partenza e arrivo

- Situazione pregressa
- Obiettivo
- Implementazione SPB
- Sostituzione NGFW
- Risultati

Situazione pregressa

60+ sedi con 1200+ reti

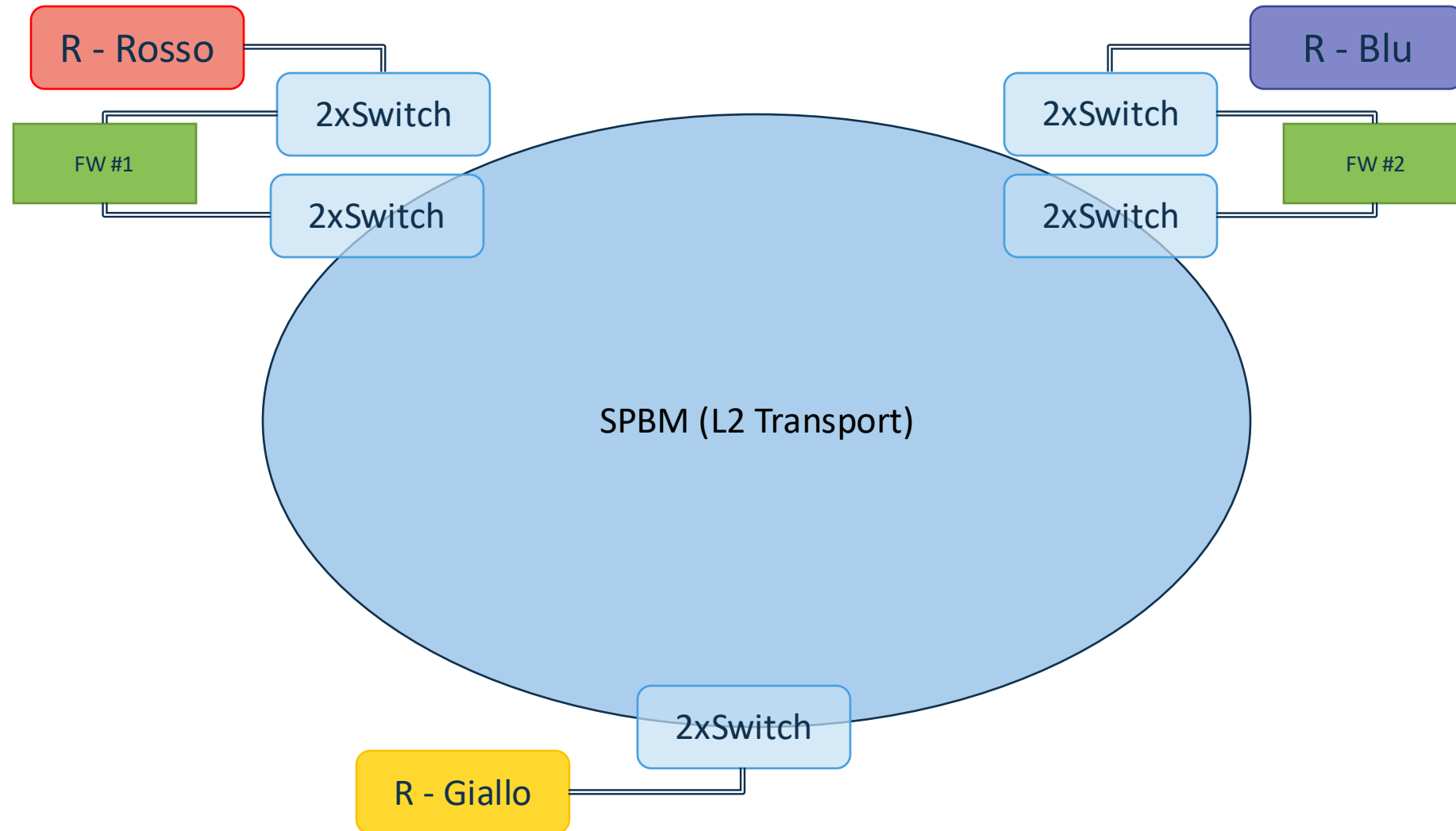
100+ router, 20+ firewall

- OSPF Multipath
- VLAN progettate su criteri geografici
- Inspection parziale del traffico laterale

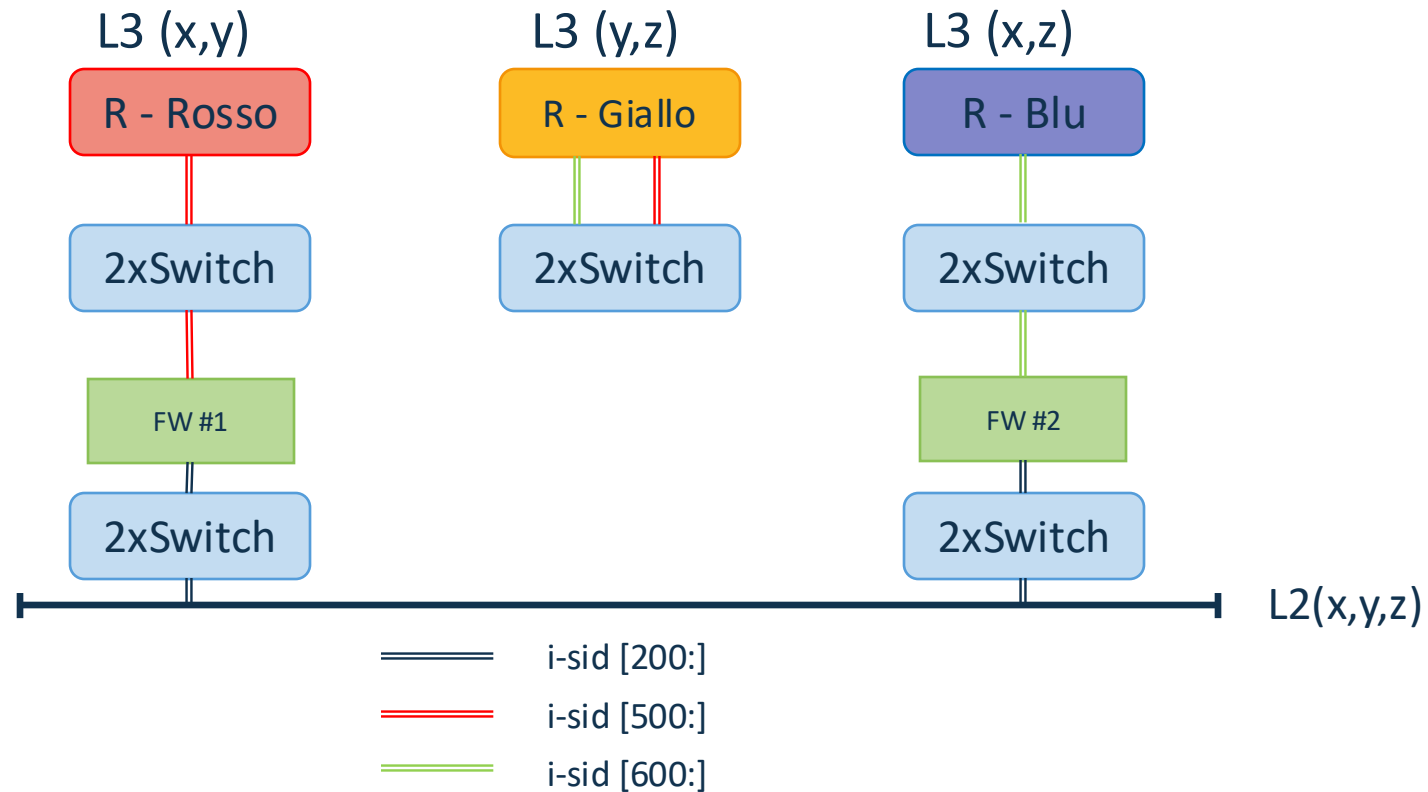
Obiettivo

- Minimizzare costi di gestione, controllo e manutenzione di router e firewall
- Vincoli:
 - Numero invariato di sedi e reti
 - Introdurre controllo traffico laterale
 - Separation of duties
- Come?
 - Distribuzione L2 geografico
 - Ridondanza VRRP
 - Firewall in virtual wire

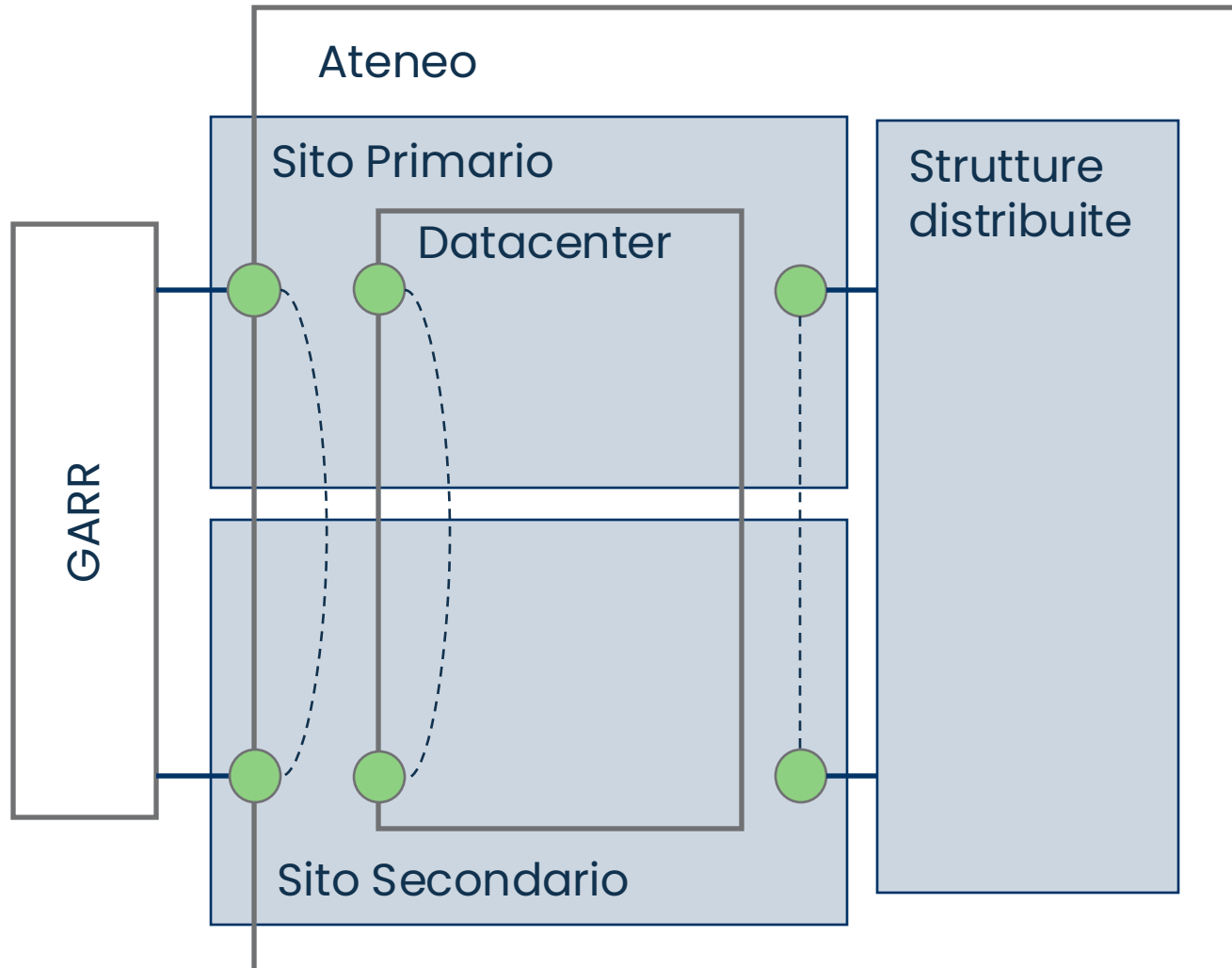
Implementazione SPB - Layout



Problema: tre router, due Firewall?



Architettura di Sicurezza



- Ridondanza
- HA Active/Active
- Controllo centralizzato

Monitoraggio del traffico laterale

- Conformità
- Prevenzione e rilevazione di attacchi inter-strutturali
- Sicurezza dei servizi con funzionalità più o meno avanzate
 - Esempio: esami universitari informatizzati
 - Interfaccia per amministratori di aula
 - Permessi differenziati per studenti e docenti
 - NAT
 - BYOD? Strumento necessario, ma non sufficiente!

Servizi sul traffico laterale

Eduroam

Aule informatizzate

Dipartimenti con esigenze speciali

Laboratori di analisi

Dipartimenti

Centri

Direzioni

Biblioteche

Residenze

Conclusioni

Bello.

- Funziona 🎉
- Tutto è più semplice
- Gestione labeling e 'trucchi per la rinumerazione'
- Pochi comandi per le attivazioni
- Doppi apparati: aggiornamenti senza interruzione di servizio

Conclusioni

Brutto?

- Non è tutto così semplice, bisogna pianificare
 - Attenzione ad evitare loop dirompenti
 - Proliferazione mac address per alcune situazioni
- L'autosensing, spesso il male
- Forward error correction... Davvero?!
- L7 e traffico asimmetrico, abbandonate ogni speranza

Grazie per l'attenzione!

Per le domande:

wooclap.com

Codice: **WSGARR25**



giancarlo.galluzzi@unimi.it

luca.giuliani@unimi.it

WORKSHOP GARR 2025

NET MAKERS