Gruppo Security - Topologie di rete

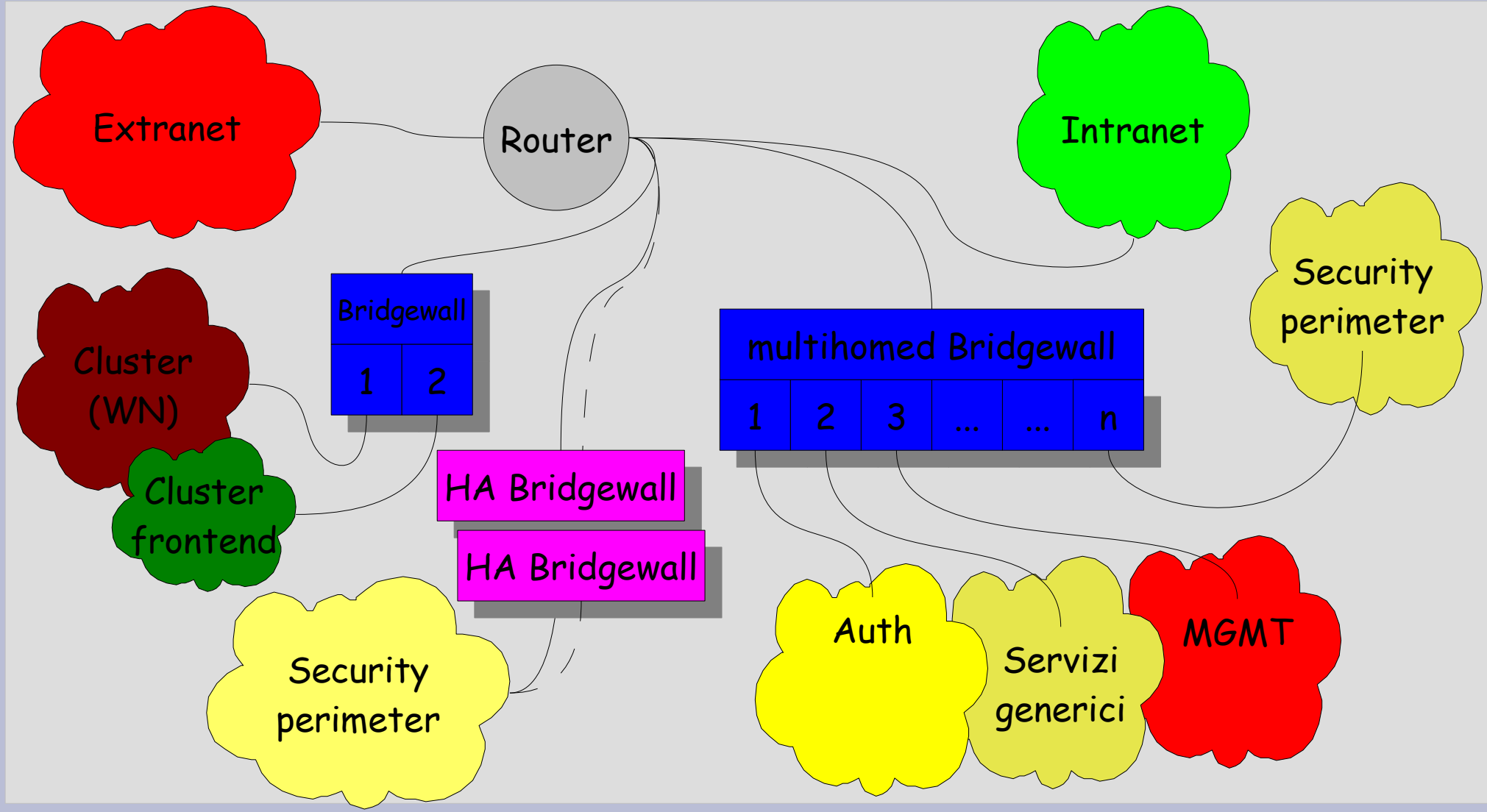
Alfieri, Belluomo, Carbone, Covati

- Programma:
  - ...
  - definizione di strumenti e topologie standard che coprano la maggioranza dei siti INFN;
  - formulazione di proposte implementative;
  - ...
- Problema: definire strumenti per implementare una security policy tale da aumentare la sicurezza senza sacrificare (troppo) le prestazioni ed affrontare pesanti ristrutturazioni; minimizzare la possibilita' di effetto domino ed il numero di punti di controllo/auditing.

Possibile (forse unica) soluzione

- **BRIDGEWALL = BRIDGE + FIREWALL**
  - stealth/transparent firewalling tramite apparato di livello 2 (**invisibile = inaccessibile**) con funzionalita' di inspection/filtering ai livelli 3,4,...,7 della pila OSI
  - implementabile con:
    - soluzioni Open Source (Linux/*BSD bridge + ebtables/arptables/iptables/ipset/nf-hipac...)
      - Testata in semi-produzione a MiB
    - soluzioni proprietarie (Cisco, Juniper, SonicWALL)
      - Costose, ma interessanti e ricche di funzionalita' esotiche (virtual firewalls, etc.)

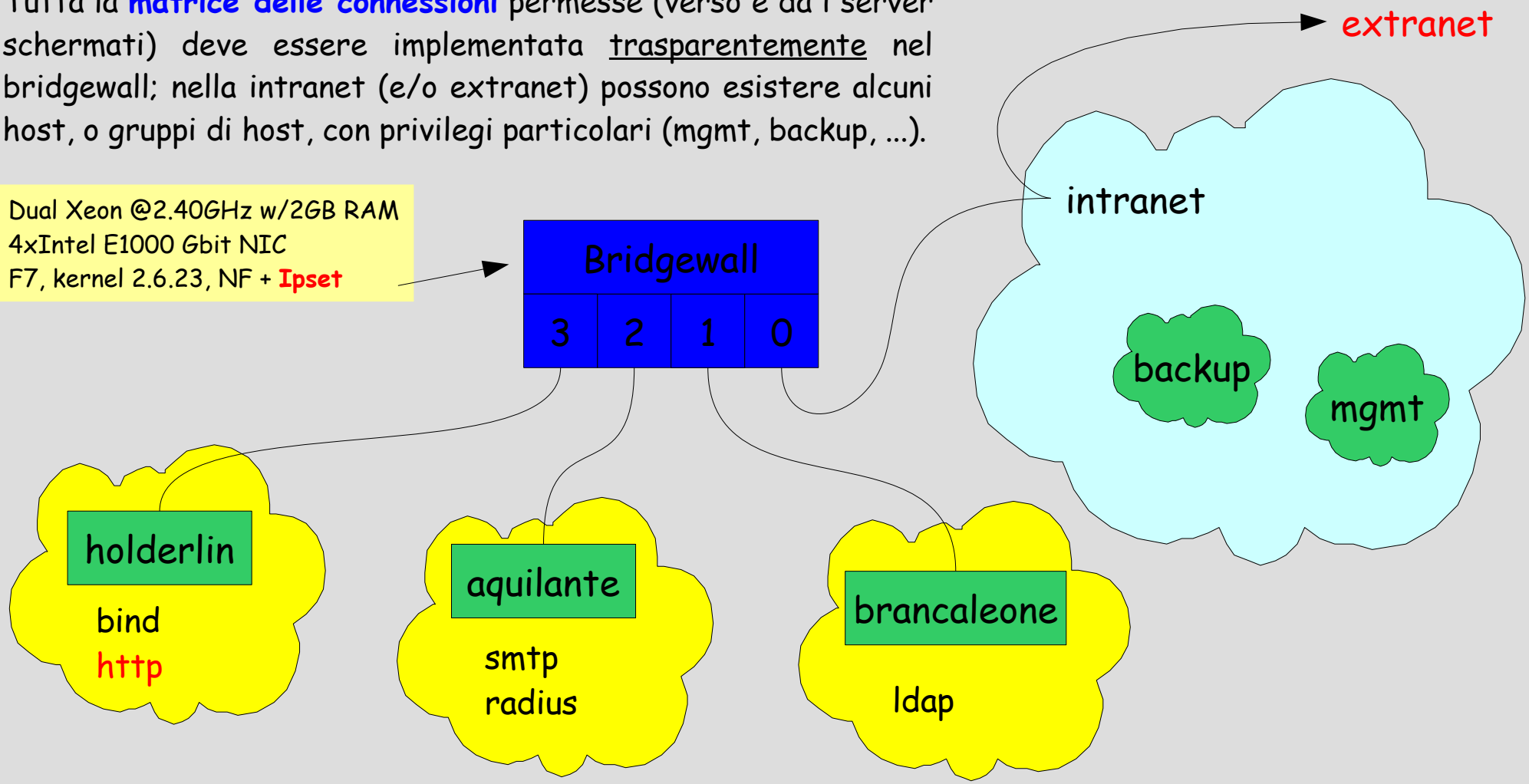
Topologie possibili



Linux BW testbed: separazione/isolamento servizi

Tutta la **matrice delle connessioni** permesse (verso e da i server schermati) deve essere implementata trasparentemente nel bridgewall; nella intranet (e/o extranet) possono esistere alcuni host, o gruppi di host, con privilegi particolari (mgmt, backup, ...).

Dual Xeon @2.40GHz w/2GB RAM
4xIntel E1000 Gbit NIC
F7, kernel 2.6.23, NF + **Ipset**



Performances: proprietary solutions vs LBW

	Cisco ASA 5520	Juniper NetScreen 208	SonicWALL PRO 4060	LBW
Max firewall throughput (Mbps)	450	375	300	930
Latency (microSec)	?	?	?	75 - 100
Max connections	280000	128000	524288	>262144
Max connections/second	9000	11500	5000	21000
Integrated ports	4x10/100/1000+1x10/100	8x10/100	6x10/100	*
Expansion slot	yes (4GE, CSC, AIP)	no	no	*
L2 transparent firewalling	yes	yes	~yes	yes
Sec. contexts/zones - VFW	2 - 20 (licensed feature)	8 - 18 (upgrade)	yes (PRO1260: 24!!)	-
Stateful HA support	Act/Act & Act/Stb	Act/Act & Act/Stb	Act/Stb	Act/Stb
Price	10.1k (4GE: ~6.3k)	11.5k	???	1.5k

CSC: Content Security & Control
AIP: Advanced Inspection & Prevention

bridge + conntrack + netfilter

To Do

- altri test (Opteron, quad-core, policy dinamiche, HA-conntrackd,...: volontari?)
- ottimizzazione SO/kernel; script per creazione device/regole (quasi fatto);
- test in produzione ***vera*** a MiB (LDAP + mail + public login) per fine 2007/inizio 2008;
- test su cluster grigliato in produzione?