Evolution Infrastructure WAF/LB/RP

AVALANCHE L4-I7

ISSUES

The existing security infrastructure consists of:

- Web Application Firewall iSentry of DenyAll
- Radware Alteon Load Balancer
- Apache Reverse Proxy

Interoperability between components

- Settings (timers, release of TCP sessions in hashing tables)

Capacity Planning

- Performance limits of the existing infrastructure

Improving the impact of this below in the application response time

Project development towards integrated solution F5

- Integration features WAF / LB / RP
- Limitation interoperability problems
- Performance increase to absorb the future burden

- PoC proposal with material BIG-IP 8900
- Performance testing with your injector HTTP / HTTPS traffic Spirent Avalanche

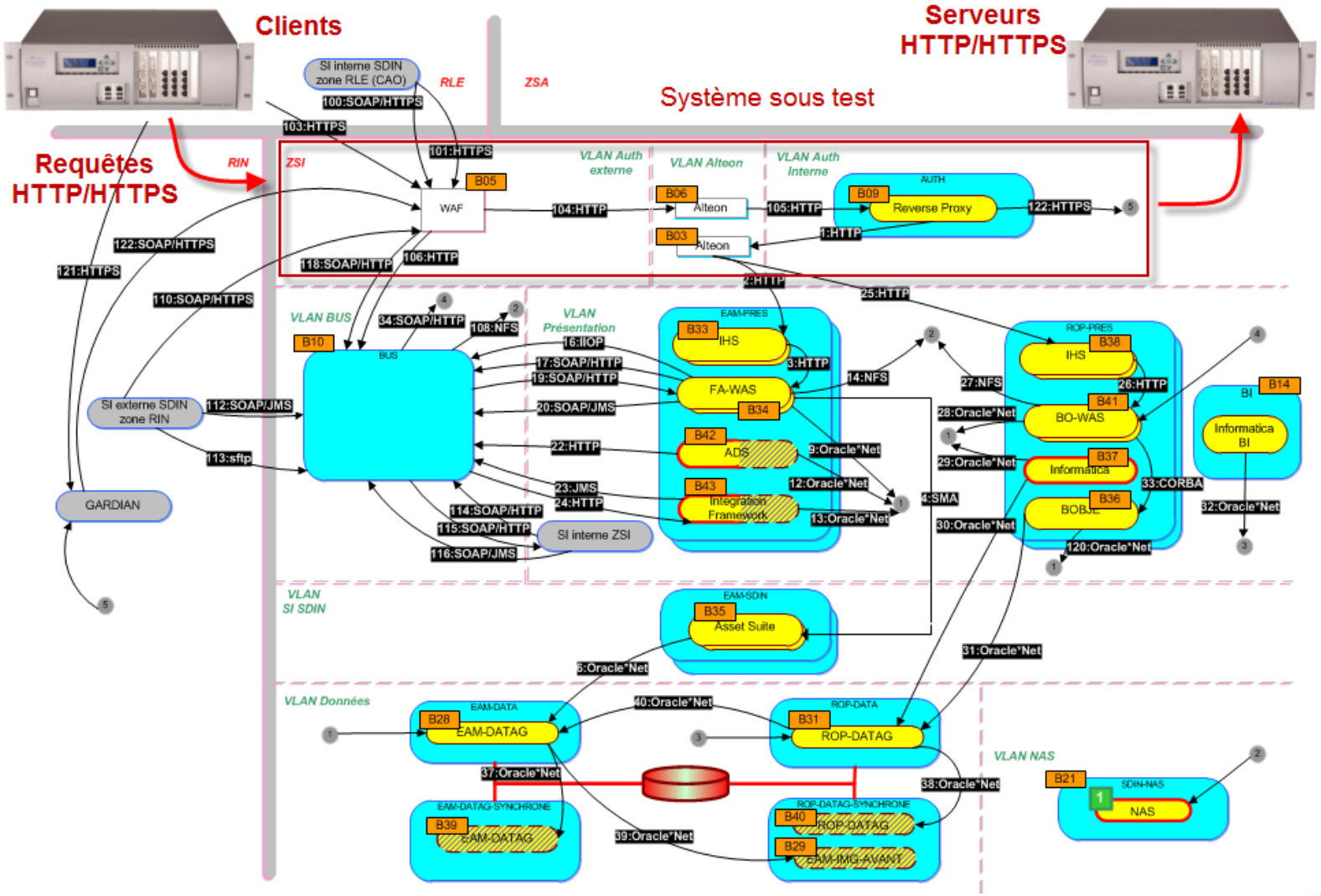
Answers to the issues

- Perform the tests to establish an inventory of performance levels of existing infrastructure, and the same tests with the new F5 solution in order to compare the results.
- Interoperability between components
  - The answer: Endurance test 8 to 12 hours & Testing High-available (measuring convergence time)Capacity Planning
  - Answer: Max Perf following RFC-3511 (CPS / TPS / OPEN / BW)
- Improving the impact of this below in the application response time
  - The answer: Creating charts with measures response times for x, y, z concurrent users

Details of the proposed tests

Validation Infrastructure Réseau

- Tests en mode Client-Serveur :



Test of endurance

- Validate the robustness of the architecture via the endurance test(8 to 12 hours)
  - Validate interoperability between components (good parameterization)
  - Check what can happen when there is eg log rotation, automatic sauvegarde, or other phenomena occurring in the systems (often at night)
  - All these phenomena are not detectable during load testing campaign with iterations of 15 minutes
  - Using a bandwidth test at 70% of the maximum load and realism (see RFC-3511)

Validation of the « high-availability »

- Validation of the mechanisms backup and failover and check how different traffic are affected when these mechanisms are activated.
- Creation of the following two types of failures :
  - Break a link (by manually unplugging),
  - Switch off equipment (to simulate a power failure)
  - Test two switchovers: when creating the fault and during the recovery (Active / Passive)..
- Measure the impact on application traffic monitoring with response times and failed transactions
  - Using a test of transactions per second, but with a charge of 50% of the identified breakpoint at maximum performance tests of RFC3511.

SPIRENT

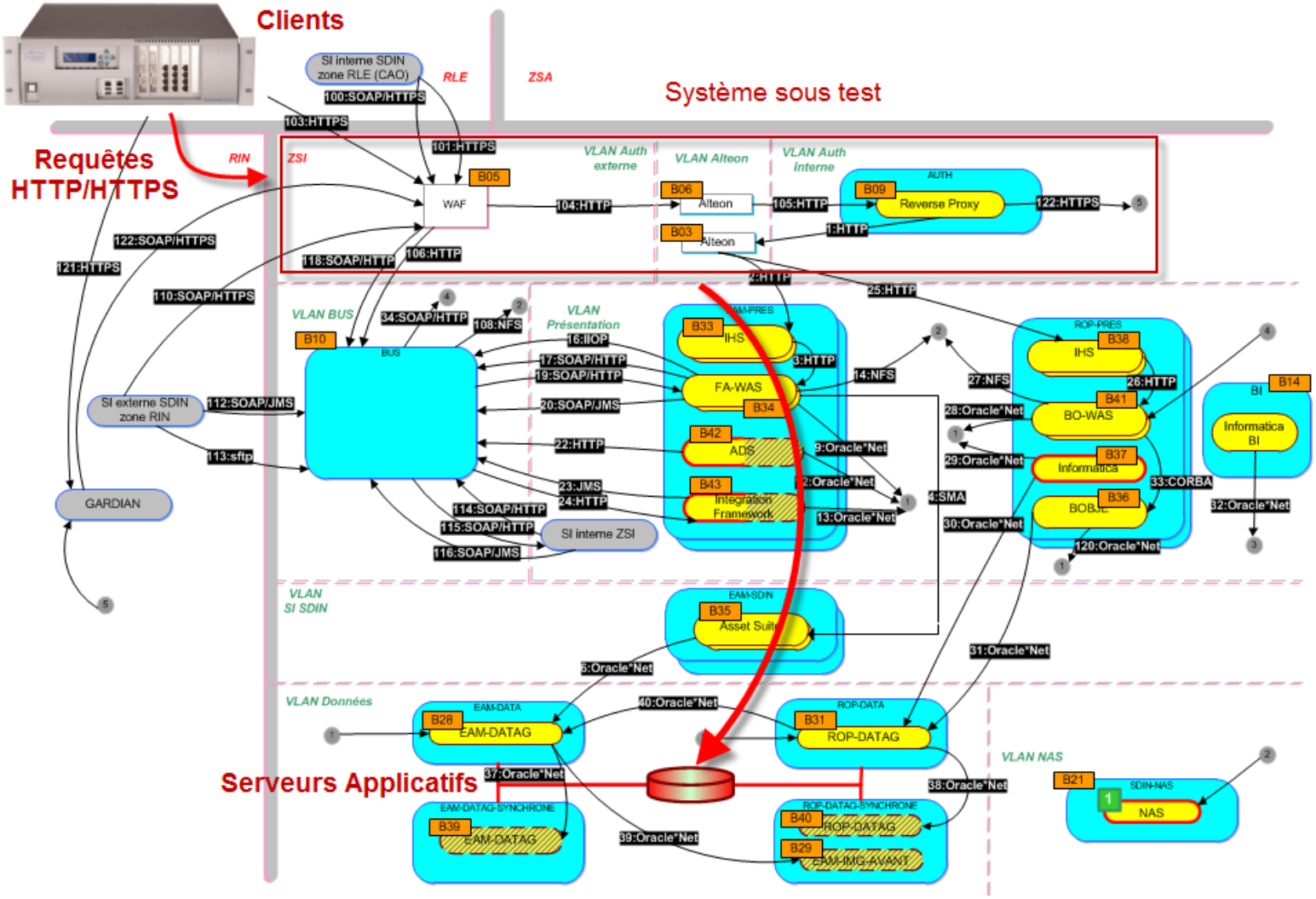
Maximum performance tests following the methodology of RFC3511 tests

- Search for the maximum number of new TCP connections per second,
- Search for the maximum number of open TCP connections simultaneously,
- Search for the maximum number of new HTTP or HTTPS transactions per second,
- Validation of the maximum bandwidth in HTTP or HTTPS.

SPIRENT

Validation Infrastructure Applicative

- Tests en mode Client-only:



Testing the end-to-end application

- Creating Clients scenario
  - Using Fiddler (proxy recorder)
- Variabilisation scenarios
- Testing scalability with monitoring response time