

Analyze | Assure | Accelerate™

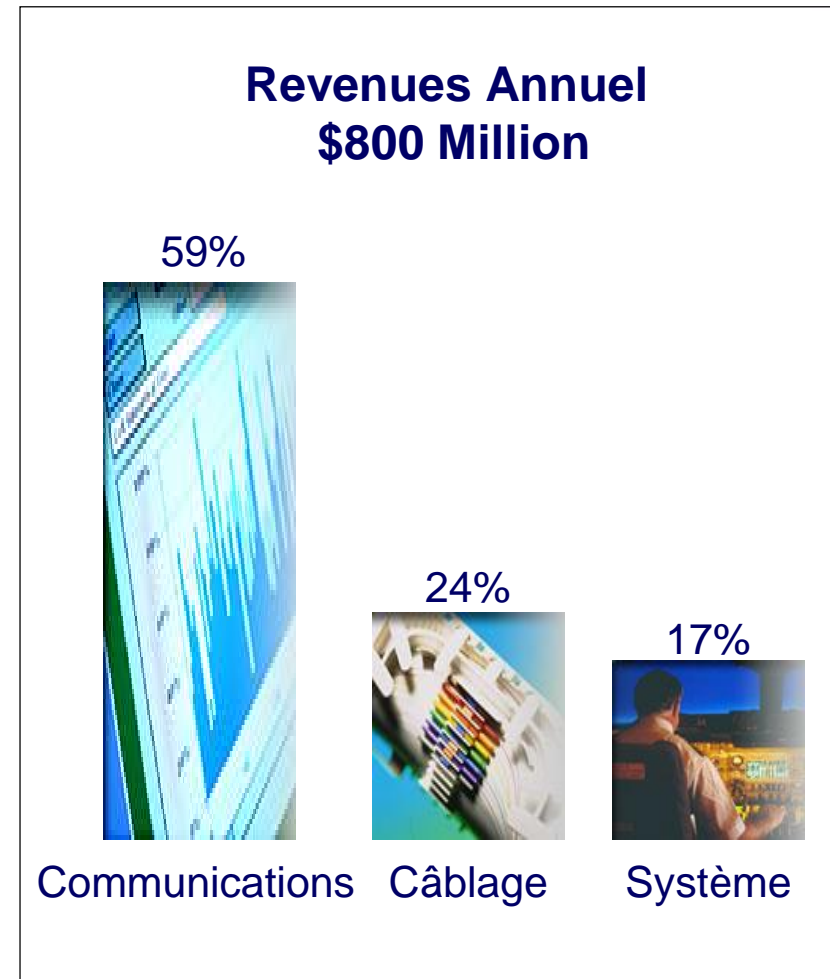
Comment valider et optimiser les performances d'un firewall ?

Antoine GAUTIER
Ingénieur Technico-Commercial
COMERIS
agautier@comeris.com

Gregory FRESNAIS
Business Development EMEA
Spirent Communications
gregory.fresnais@spirentcom.com

Spirent

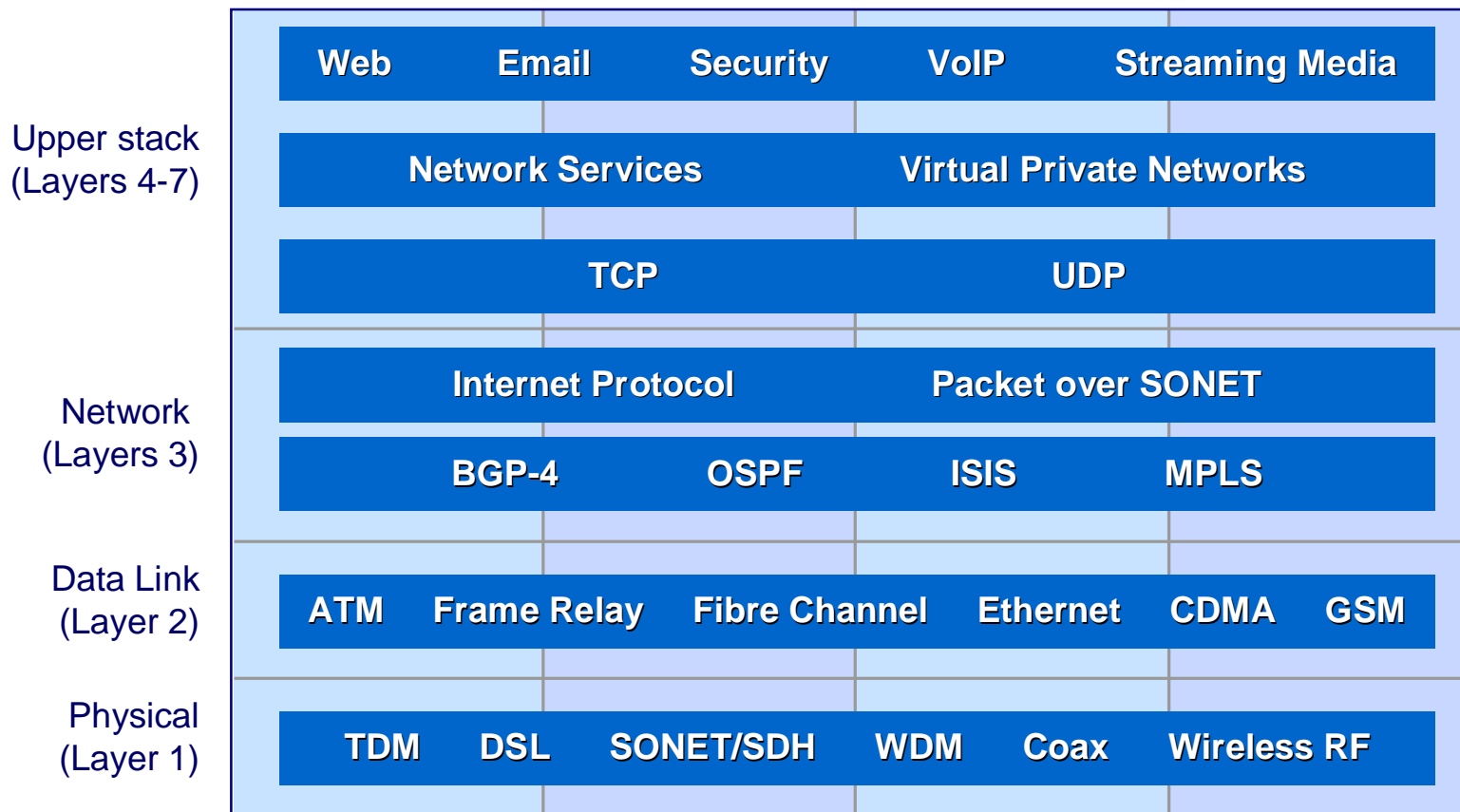
- Compagnie internationale
 - ∅ Siège en Angleterre.
 - ∅ Présence mondiale.
 - ∅ Plus de 4000 employées.
- Trois divisions principales
 - ∅ Communication
 - Équipement de test.
 - ∅ Câblage
 - Câbles et connections réseaux.
 - ∅ Système
 - Logiciel de navigation,



Équipement de Test

Business: Enterprise . Financial . Government . Telco . xSP . Mobile operator . NEM

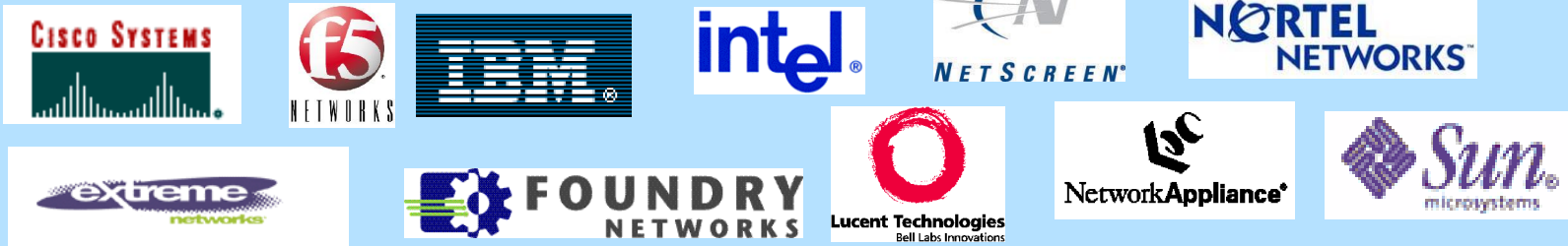
Layer : Research . Development . Network testing . Application testing . Service testing



Nos clients

Nos clients

Network Equipment Manufacturers



Network Service Providers



Enterprise & Government



Agenda

- Problématique des Firewalls au déploiement
- Comment valider les performances de son Firewall ?
- Validation des performances du Firewall
- Optimisation des performances du Firewall
- Les autres possibilités de la solution

Problématique des Firewalls au déploiement

- Assurer la sécurité des données de l'entreprise
- Assurer la sécurité des utilisateurs
- Garantir la qualité de service
- Choisir son firewall

Sécurité des données

- Analyser les protocoles utilisés
- Connaître les personnes autoriser
- Pour quel type de service ?

Sécurité des utilisateurs

- Combien d' utilisateurs ? (10, 1000, 10000 ...)
- Quel type de connexion ? (Modem, ADSL ...)
- Avec quel moyen d'accès (Navigateur Web, Pda, Mobile...)
- Pour quel type d'application ? (Web, Messagerie, Serveur de fichier...)
- Avec quel niveau de sécurité ?(SSL, IPSec, HTTPS ...)

Garantir la qualité de Service

- Déterminer la bande passante nécessaire
- Déterminer les temps de réponses utilisateurs (réseaux, applications)
- Vérifier la qualité de l'information retournée

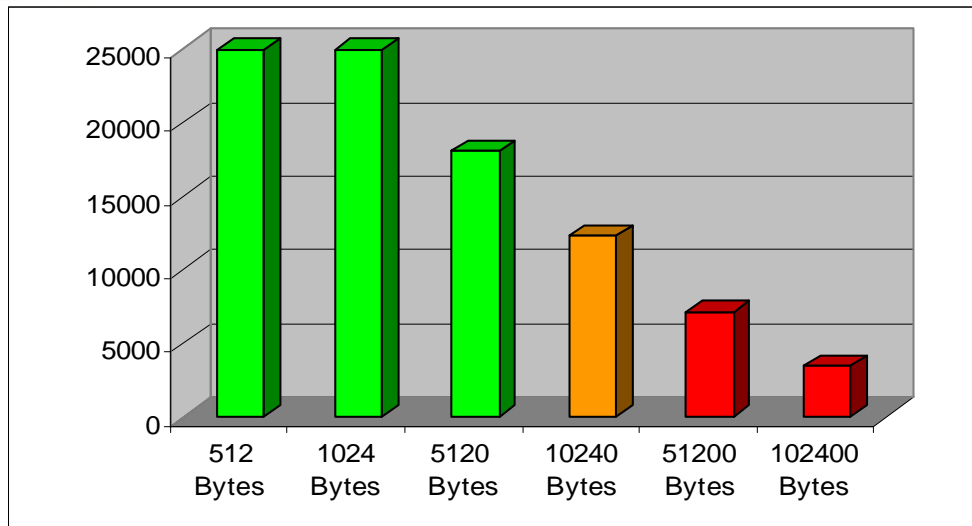
Choisir son Firewall

- Quel type de Firewall ? (Appliance, logiciel)
- Avec quelle performance ?
- En quelle quantité ?
- Disponibilité ?

Comment valider les performances de son Firewall ?

- Méthodologie des tests
- Choix du Firewall
- Performance du Firewall
- Optimisation du Firewall

Dégradation des Performances d'un Firewall



Comparaison des performances des firewalls: Téléchargement d'un fichier de 1 Ko

Qui déploie un site web avec des pages HTML de 1024 Bytes ?

Seuil d'Acceptabilité

- ü Maximum TCP Connection Rate > 15 000 TCP/SEC ■
- ü Maximum TCP Connection Rate > 15 000 and > 10 000 TCP/SEC ■
- ü Maximum TCP Connection Rate < 10 000 TCP/SEC ■

Point de Rupture

- ü Maximum Response Time for Request at Layer 7 = 100 ms
- ü Maximum Concurrent TCP Connection at Layer 4 = 200
- ü Maximum Bandwidth use under 70% of maximum available

Méthodologie de test

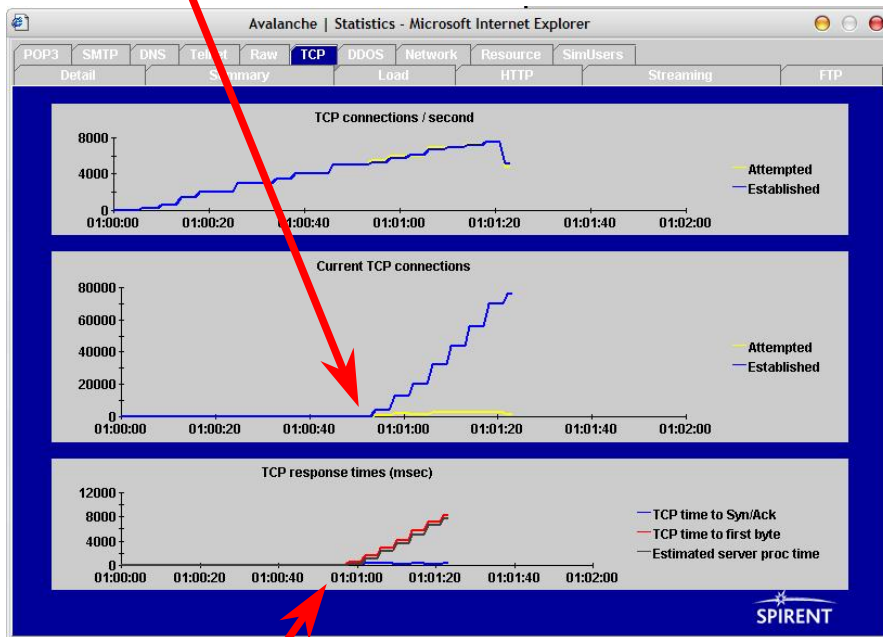
- Tests fonctionnels
 - ∅ Valider les règles du Firewall pour peu d'utilisateurs
- Tests de performances
 - ∅ Maximum de connections TCP par seconde
 - ∅ Maximum de connections TCP maintenues ouvertes
 - ∅ Maximum de transactions HTTP par seconde
 - ∅ Maximum de bande passante disponible
 - ∅ Protection contre des attaques de niveau 2 a 4
 - ∅ Protection contre des attaques de niveau 7

Test 1 – Performance TCP/SEC

- Validation du maximum de nouvelles connections TCP par seconde – 6 Tests
 - ∅ Configuration du Client: HTTP 1.0 utilisant 1 transaction HTTP dans 1 connection TCP
 - ∅ Validation avec des pages HTML en bytes: 512, 1024, 5120, 10240, 51200, 102400
 - ∅ Configuration du Serveur: HTTP 1.0, fermant la connection TCP après 1 transaction HTTP
- Point de Rupture avec prise de performance quand:
 - ∅ Temps de réponse pour une transaction HTTP dépasse 100 ms
 - ∅ 1 transaction HTTP est en échec
 - ∅ Nombre de connection TCP maintenue ouverte dépasse 200

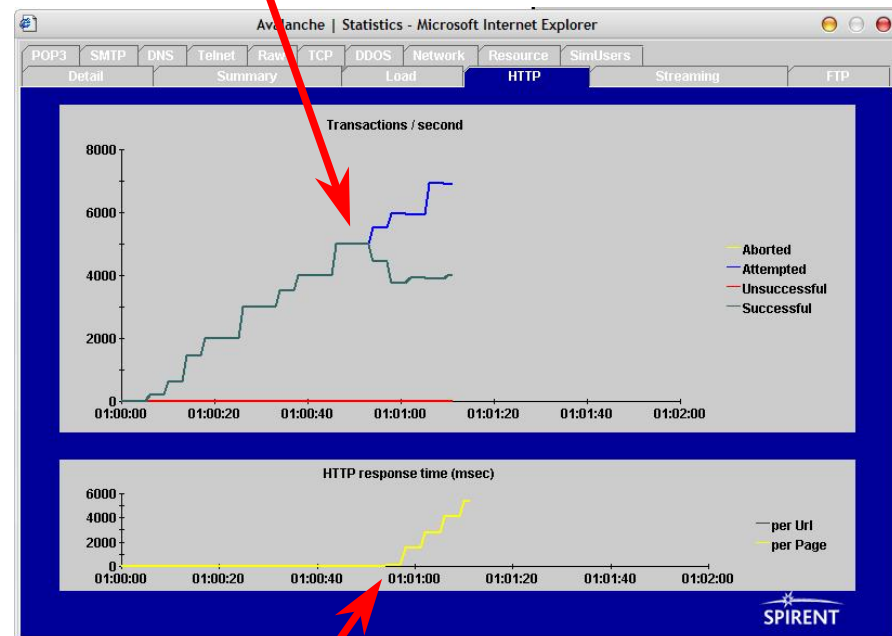
Test 1 - Performance TCP/SEC

Connections TCP maintenues ouvertes > 100



Time to First Byte augmente

Point de Rupture



Temps de réponse pour une requette HTTP dépasse > 100 ms

Test 2 – Performance TCP OPEN

- Validation du maximum de connection TCP maintenue ouverte – 6 Tests
 - ∅ Configuration du Client: HTTP 1.1 utilisant 10 transactions HTTP dans 1 connection TCP
 - ∅ Think Time de 30 secondes
 - ∅ Validation avec des pages HTML en bytes: 512, 1024, 5120, 10240, 51200, 102400
 - ∅ Configuration du Serveur: HTTP 1.1, fermant la connection TCP après 10 transactions HTTP
- Point de Rupture avec prise de performance quand:
 - ∅ Temps de réponse pour une transaction HTTP dépasse 100 ms
 - ∅ 1 transaction HTTP est en échec

Test 3 – Performance GET/SEC

- Validation du maximum de transaction HTTP par seconds – 6 Tests
 - ∅ Configuration du Client: HTTP 1.1 utilisant 10 transactions HTTP dans 1 connection TCP
 - ∅ Validation avec des pages HTML en bytes: 512, 1024, 5120, 10240, 51200, 102400
 - ∅ Configuration du Serveur: HTTP 1.1, fermant la connection TCP après 10 transactions HTTP
- Point de Rupture avec prise de performance quand:
 - ∅ Temps de réponse pour une transaction HTTP dépasse 100 ms
 - ∅ 1 transaction HTTP est en échec

Test 4 – Performance Bande Passante

- Validation de la bande passante maximum disponible – 1 Test
 - ∅ Configuration du Client: HTTP 1.1 utilisant 1 transaction HTTP dans 10 connection TCP
 - ∅ Configuration du Serveur: HTTP 1.1, fermant la connection TCP après 10 transaction HTTP

- Point de Rupture avec prise de performance quand:
 - ∅ 1 transaction HTTP est en échec

Test 5 – Attaques de Niveau 2 a 4

- Validation des performances du Firewall sous attaques
 - ∅ TCP Syn Flood
 - ∅ TCP Port Scan
 - ∅ UDP Flood
 - ∅ UDP Port Scan
 - ∅ ARP Flood
 - ∅ Smurf
 - ∅ Ping Sweep
- Point de Rupture avec prise de performance quand:
 - ∅ Temps de réponse pour une transaction HTTP dépasse 100 ms
 - ∅ 1 transaction HTTP est en échec

Test 6 – Attaques de Niveau 7

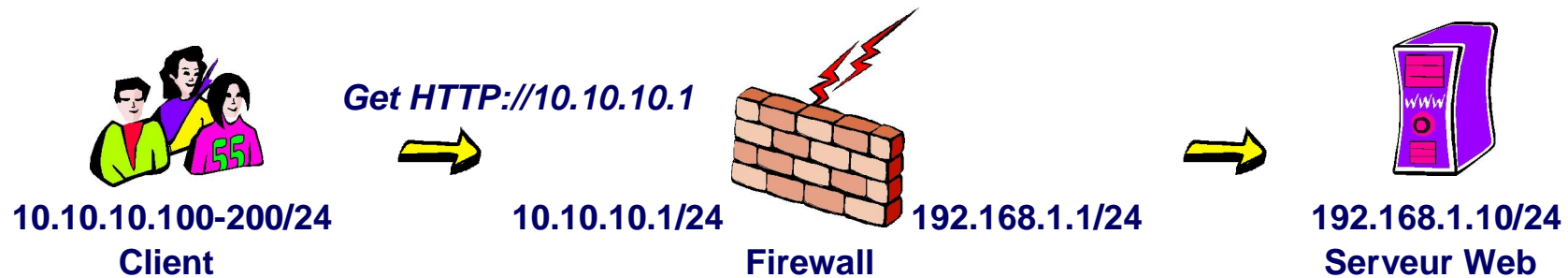
- Validation des performances du Firewall sous attaques
 - ∅ Virus
 - ∅ Attaques Applicatives (Web Server, FTP Server, Messagerie)
- Point de Rupture avec prise de performance quand:
 - ∅ Temps de réponse pour une transaction HTTP dépasse 100 ms
 - ∅ 1 transaction HTTP est en échec

Choix du Firewall

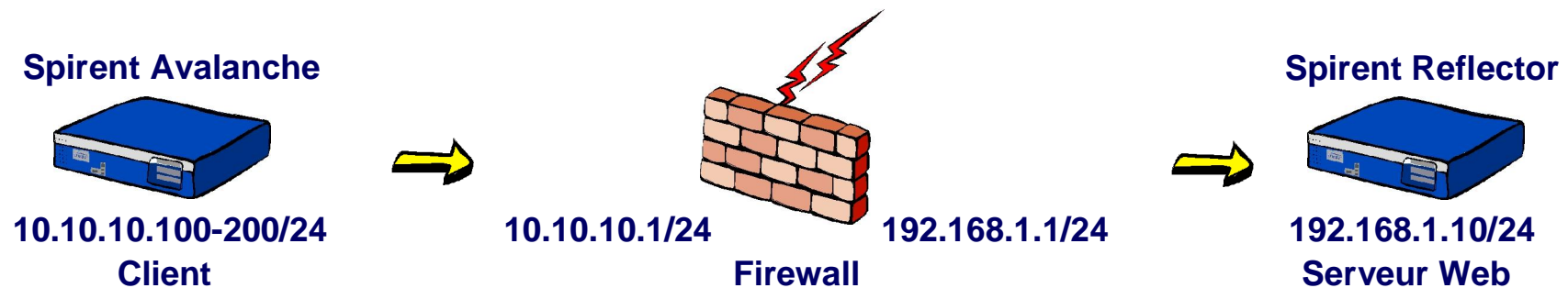
- IpTables est une solution complète de firewall (noyau 2.4) remplaçant *ipchains* (noyau 2.2) tournant sous le système GNU/Linux.
- IpTables permet de faire
 - ∅ translation de port et d'adresse
 - ∅ filtrage au niveau 2
 - ∅ Et beaucoup d'autres choses ...

Infrastructure Réseau

Infrastructure du Client



Infrastructure de test avec Avalanche et Reflector



Les autres possibilités de la solution

Prestation de service

Proposition 1 – Validation des performances réseaux

*Validation
infrastructure
réseau*

Router, Firewall, Load Balancer, Accélérateur SSL, Packet Shaper, IPS/IDS, ...

Proposition 2 – Validation des performances applicatives

*Validation
des
applications*

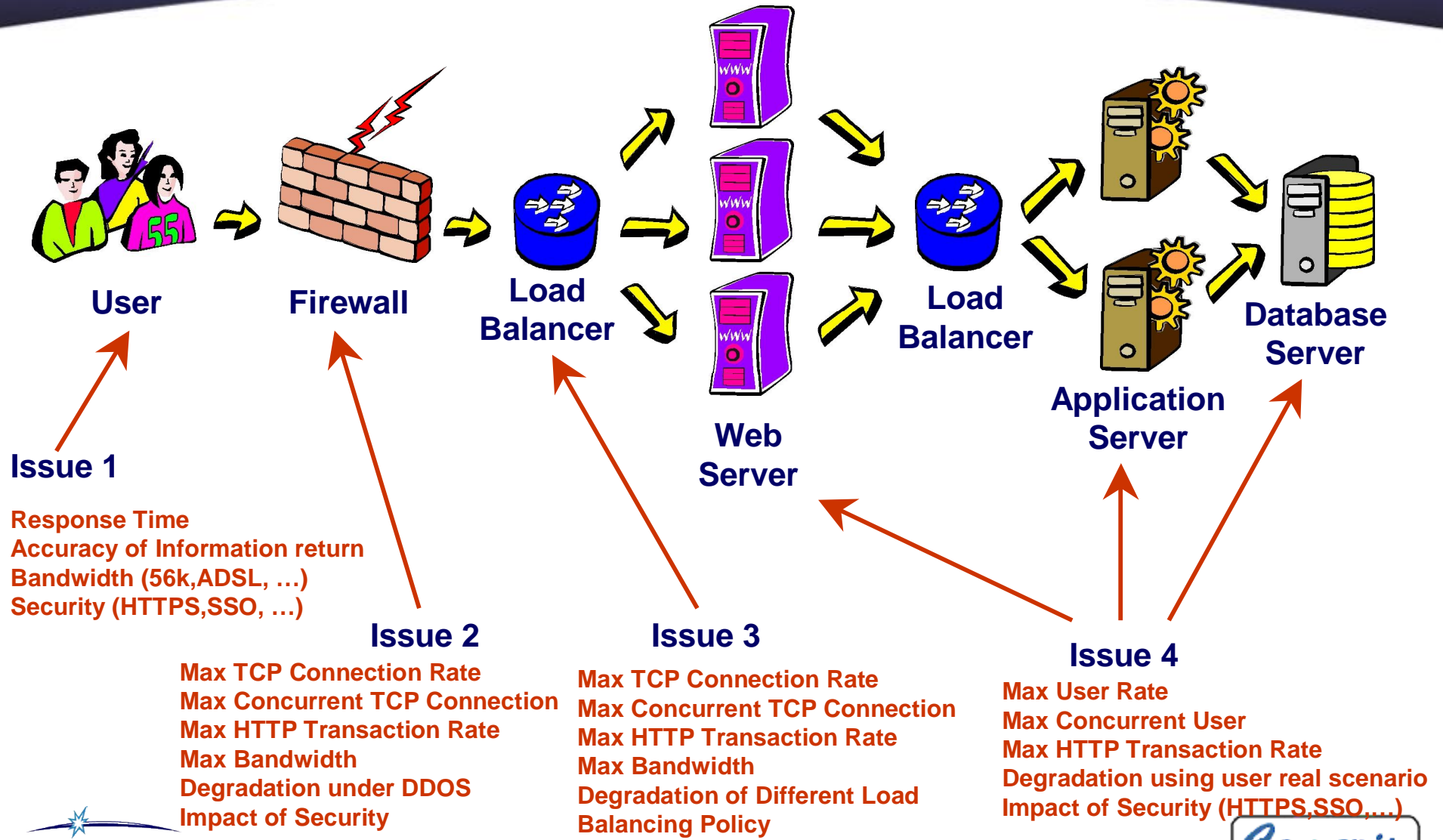
Serveur Web, Serveur DNS , Serveur Mail, Content Filter, Proxy/Cache, Accélérateur HTTP/HTTPS, Serveur de Streaming ...

Proposition 3 – Validation des performances du service

*Validation du
service*

Infrastructure 3-Tiers (Siebel, SAP, BEA, Oracle), E-commerce Web Site, Billing Platform (CISCO SESM), Video on Demand Service, ...

Site Web – Intranet



Issue 1
 Response Time
 Accuracy of Information return
 Bandwidth (56k,ADSL, ...)
 Security (HTTPS,SSO, ...)

Issue 2
 Max TCP Connection Rate
 Max Concurrent TCP Connection
 Max HTTP Transaction Rate
 Max Bandwidth
 Degradation under DDOS
 Impact of Security

Issue 3
 Max TCP Connection Rate
 Max Concurrent TCP Connection
 Max HTTP Transaction Rate
 Max Bandwidth
 Degradation of Different Load
 Balancing Policy

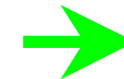
Issue 4
 Max User Rate
 Max Concurrent User
 Max HTTP Transaction Rate
 Degradation using user real scenario
 Impact of Security (HTTPS,SSO,...)

Categorisation de Problems

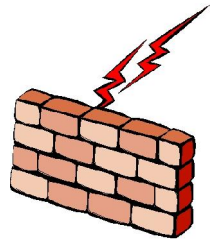


Issue 1

Response Time
Accuracy of Information return
Bandwidth (56k,ADSL, ...)
Security (HTTPS,SSO, ...)



Service Issue



Issue 2

Max TCP Connection Rate
Max Concurrent TCP Connection
Max HTTP Transaction Rate
Max Bandwidth
Degradation under DDOS
Impact of Security

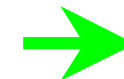


Network Issue

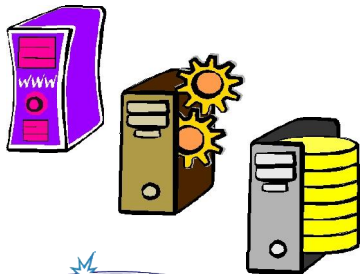


Issue 3

Max TCP Connection Rate
Max Concurrent TCP Connection
Max HTTP Transaction Rate
Max Bandwidth
Degradation of Different Load Balancing Policy



Network Issue



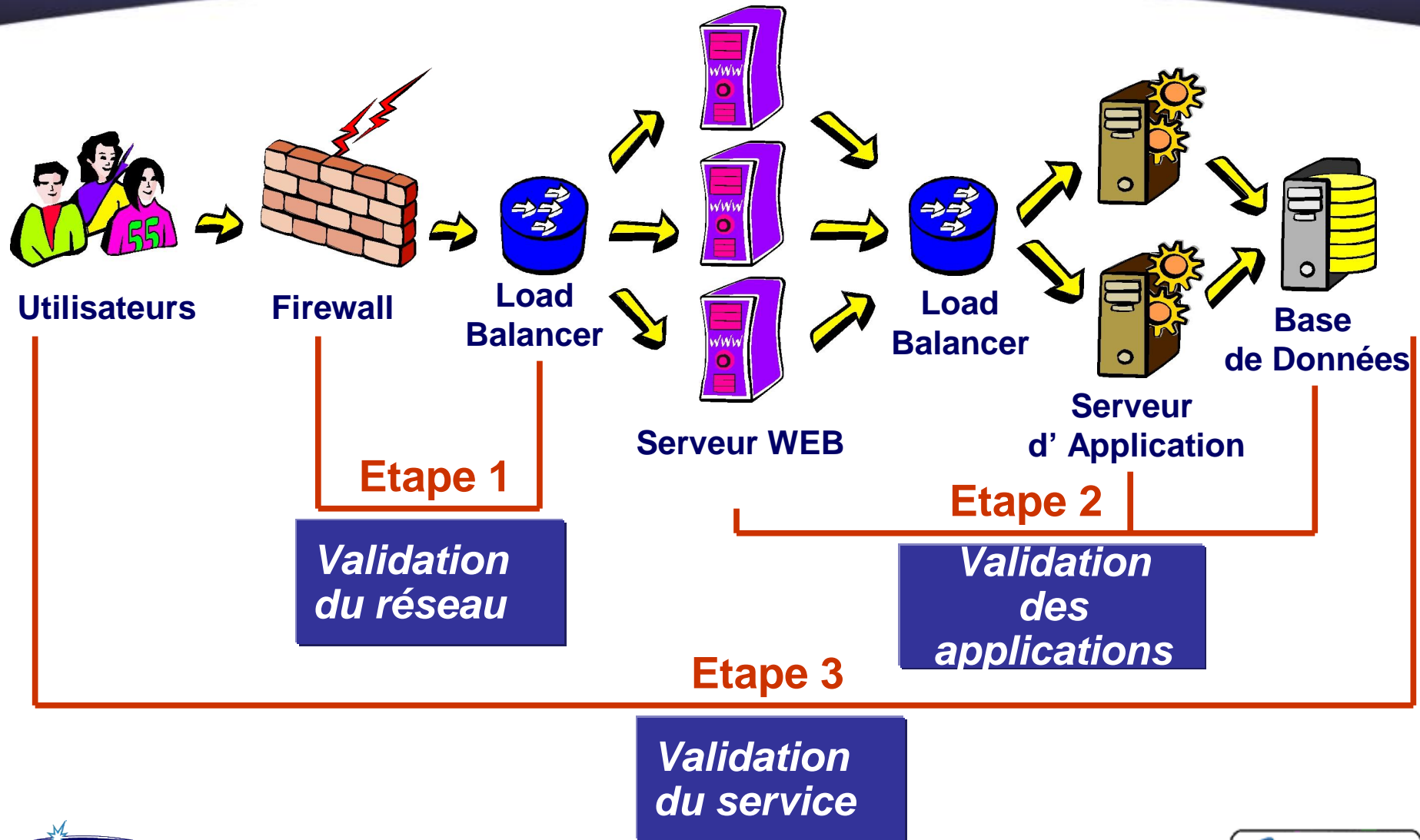
Issue 4

Max User Rate
Max Concurrent User
Max HTTP Transaction Rate
Degradation using user real scenario
Impact of Security (HTTPS,SSO,...)



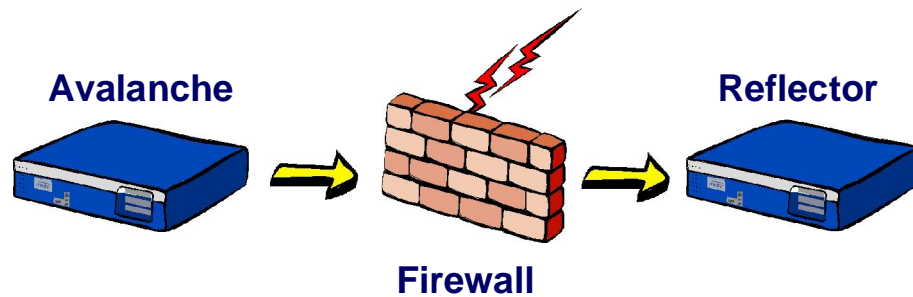
Application Issue

Étape de Validation

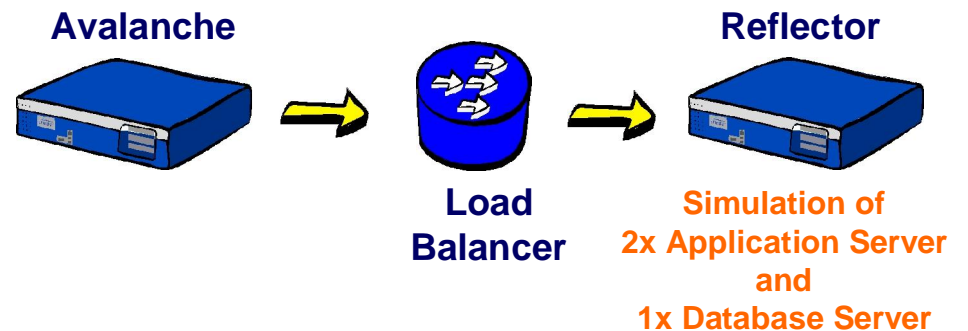


Proposition 1 - Validation du Réseau

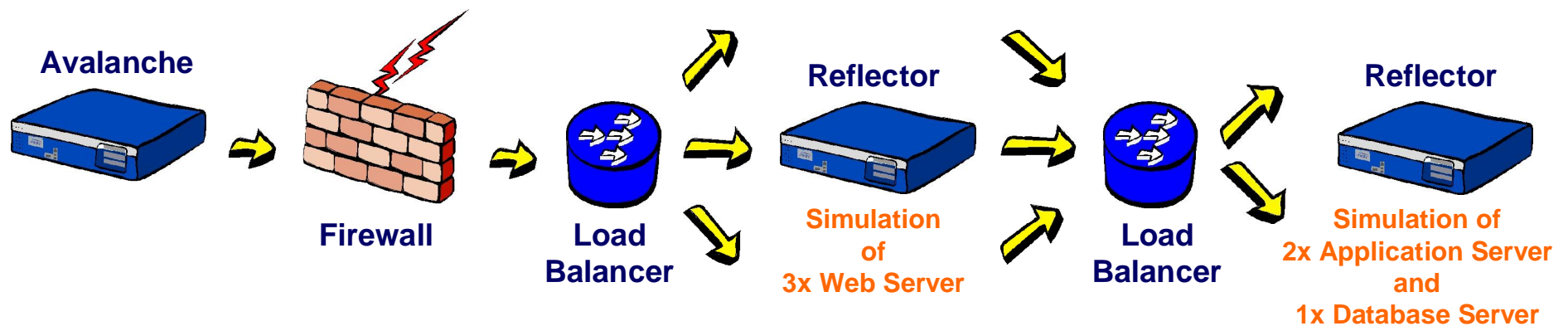
Step 1



Step 2

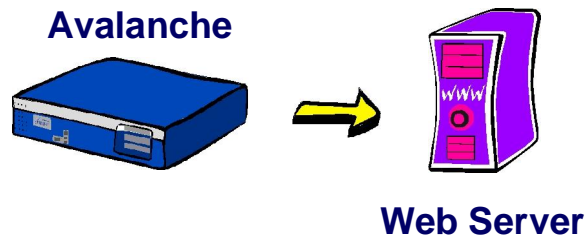


Step 3

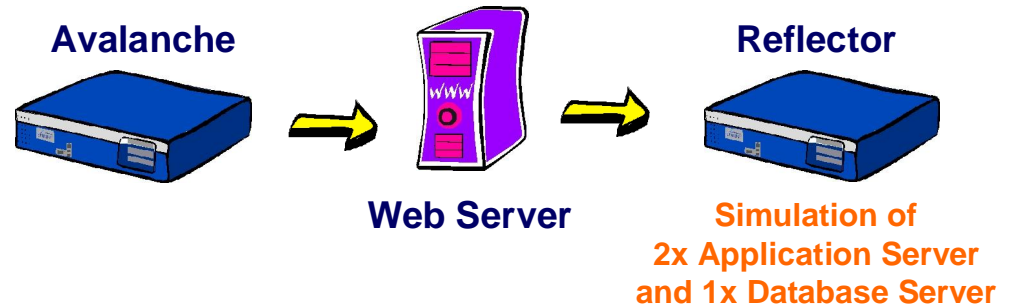


Proposition 2 - Validation des Applications

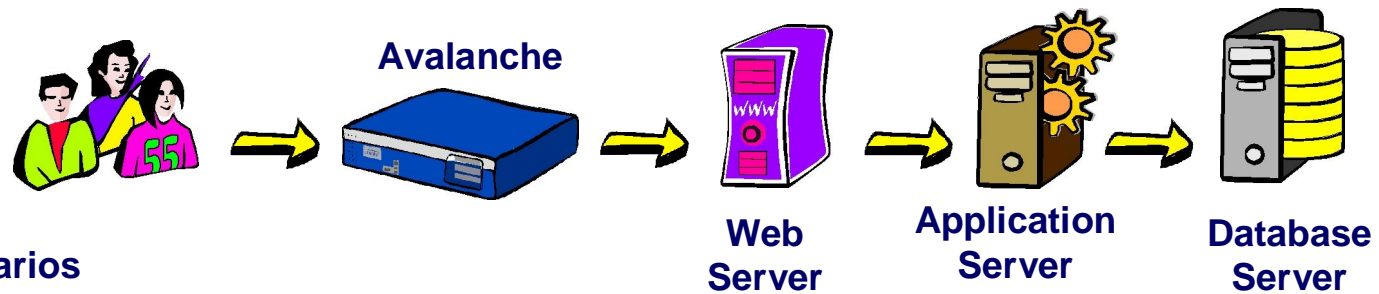
Step 1



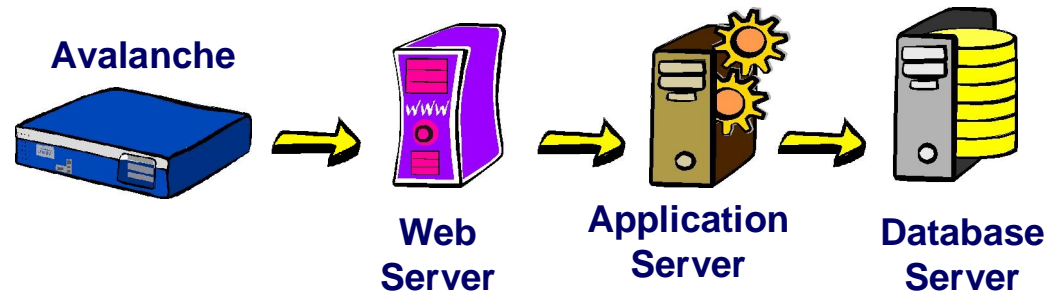
Step 2



Step 3

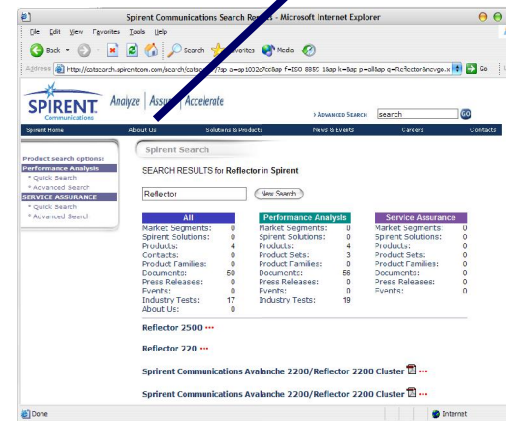
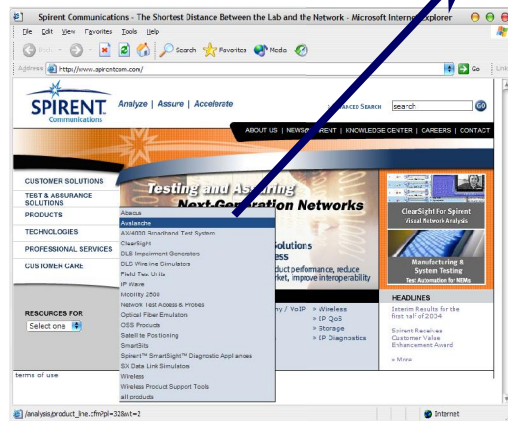
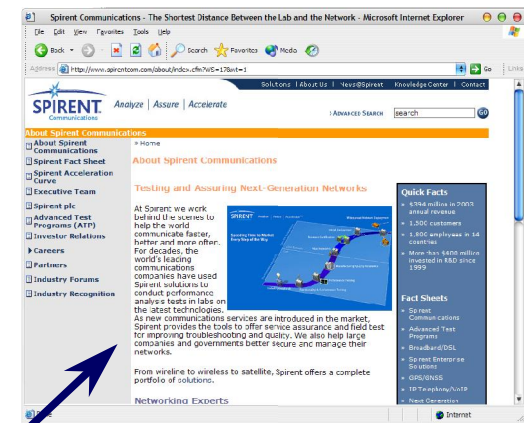
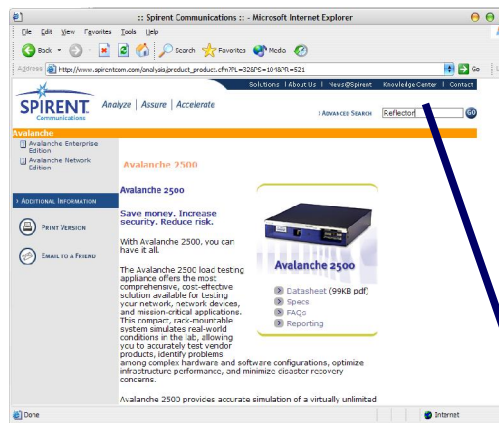
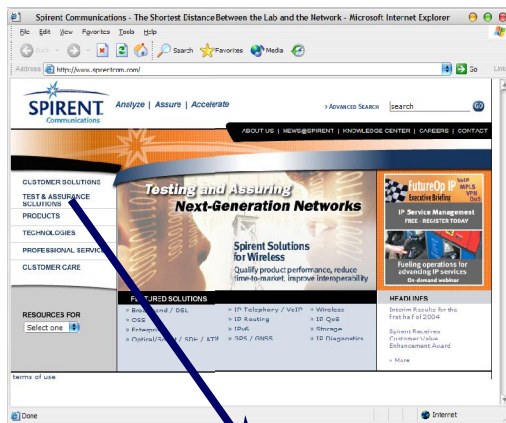


Step 4



Création de scénarios réalistes.

Etape 3 de la validation des applications



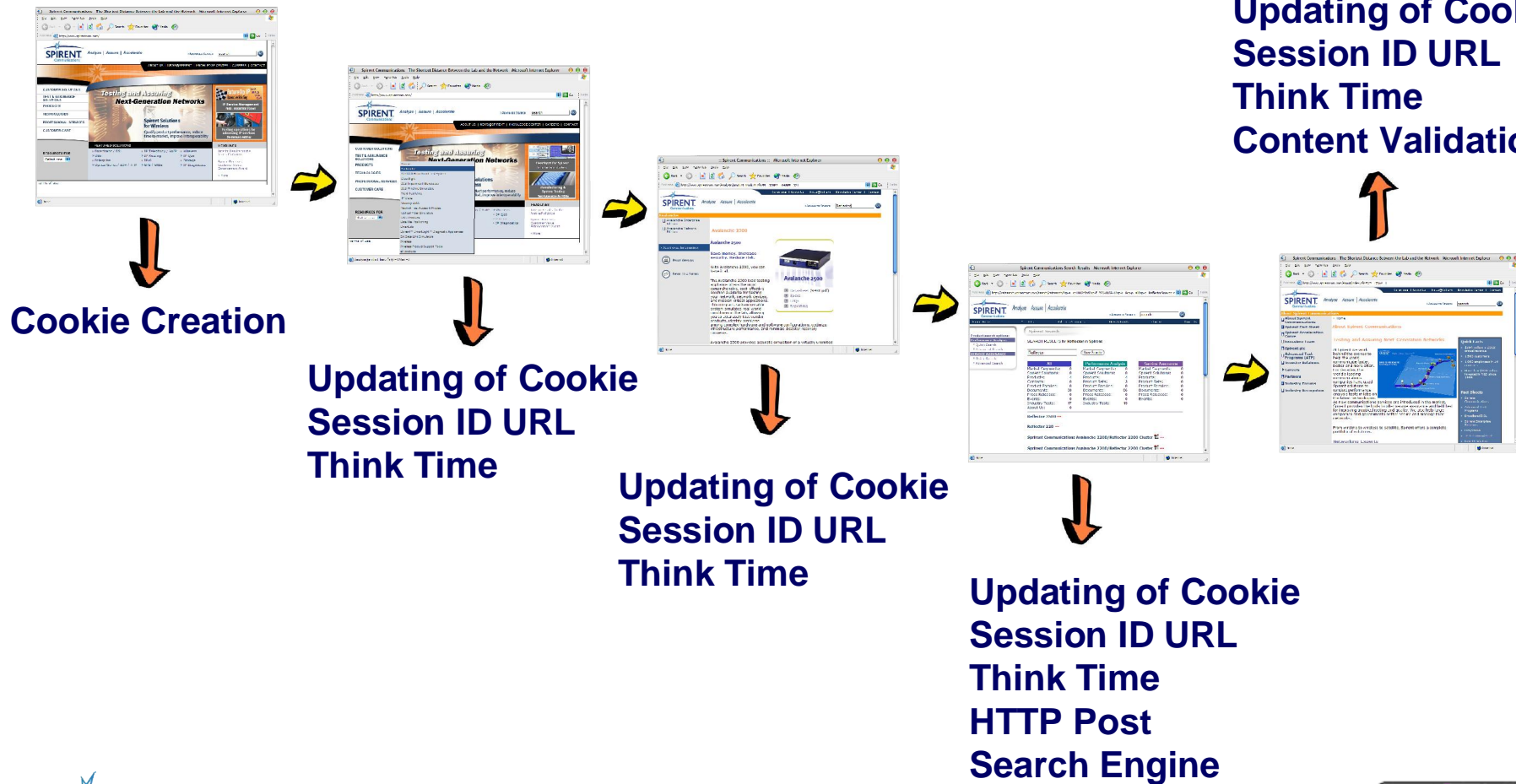
Analyze | Assure | Accelerate™

April 28, 2005



Analyses des scénarios réalistes.

Etape 3 de la validation des applications



Validation des performances du portail Web

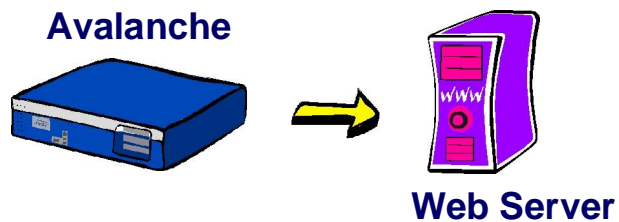
Phase 1 – Web Server Performance – 3 Tests

Phase 2 – Web Server Performance with Simulation of Application Server - 24 Tests

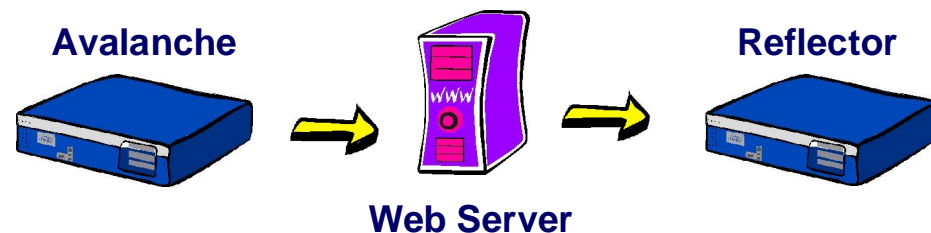
Phase 3 – Creation of Real User Scenarios - 10 Scenarios

Phase 4 – Web Portal Performance with Real User Scenarios - 10 Tests

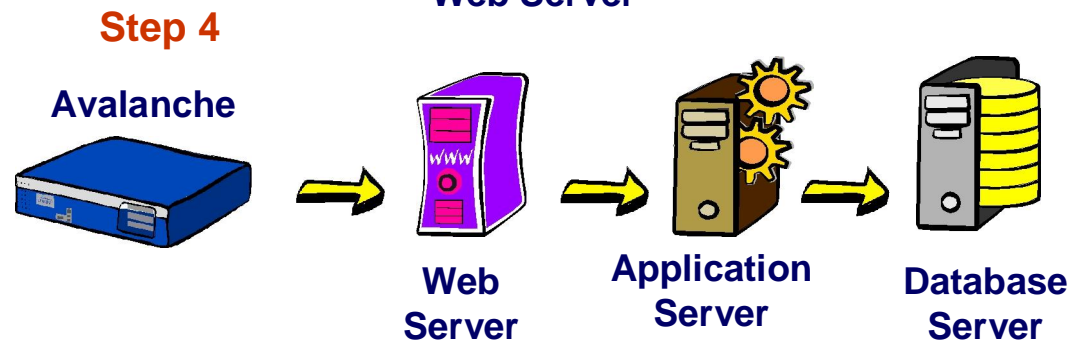
Step 1



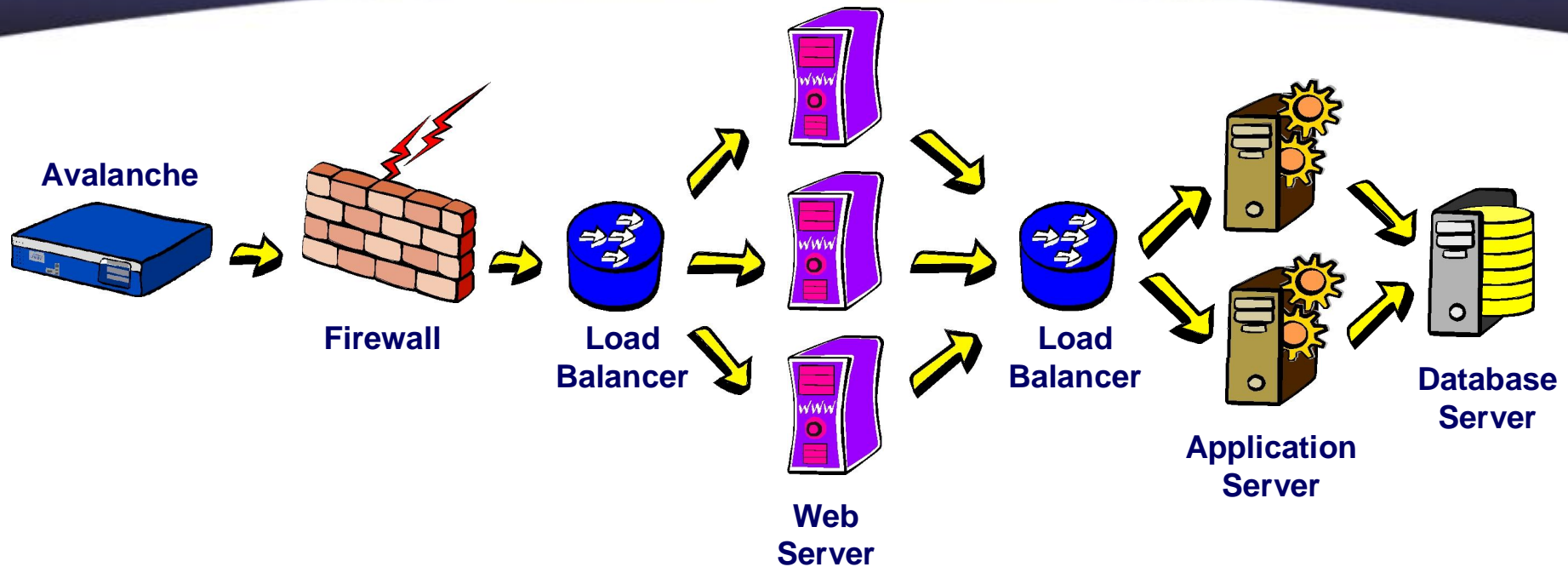
Step 2



Step 3 Creation of Scenarios



Proposition 3 – Validation du service



- Maximum New User Rate (TCP/SEC, GET/SEC)
- Maximum Concurrent User (TCP OPEN, GET/SEC)
- Assurance of Quality of Service (RESPONSE TIME)
- Correct Dimensioning in terms of Network Equipment and Servers

Professional Services - References

- NEMs – Network Equipment Manufacturers
 - ∅ Cisco, Fortinet, HP, NetScaler ...
- SPs - Service Providers
 - ∅ BT, Orange, IT Telecom, T-Online ...
- Enterprise/Government
 - ∅ Betfair, BNP Paribas, British Petroleum, Channel 4, Credit Agricole, Credit Cooperatif, Direction General Des Impots, La Poste, National Health Service, Reuters, Societe General ...

Utilisation d'Avalanche et de Reflector

Web Server

Application Server

Database Server

IDS/IPS

Packet Shaper

PPPOE

Mail Server

FTP Server

Firewall

HTTP/HTTPS Accelerator

Router

Switch

Infrastructure

Content Filtering

Cache Server

Proxy Server

DNS Server

Telnet Server

Streaming

Multicast

Anti-Virus

Denial of Service

SSL Accelerator

Web Portal

Billing Platform

MMS, WAP, LBS

....

Award winning products



Driving industry standards



Avalanche – Simulation des Clients

- Générer plus de 80,000 get/sec HTTP 1.1
- Envoyer plus de 20 000 email/sec
- Supporter HTTP, HTTPS, SOAP, FTP, DNS, Telnet, SMTP, POP3, Streaming, Multicast, Capture and Replay, DDOS Attacks
- Supporter VLAN Tagging et IP Fragmentation
- Générer plus de 8 000 sessions SSL par sec.
- Maintenir plus de 2 millions de connections TCP
- Capable de soutenir un trafic de 2.6 Gbits/sec
- Statistiques en temps réel



220

"An ISP in a box"

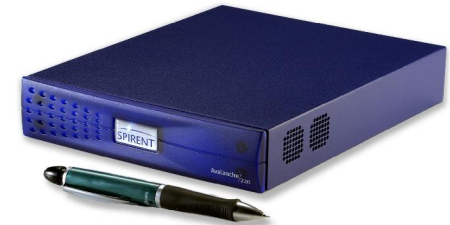
SmartBits



2500

Reflector – Simulation des Serveurs

- Support des protocoles suivants: HTTP, HTTPS, SOAP, 220 FTP, DNS, Telnet, SMTP, Pop3, Streaming, Multicast, Capture and Replay
- Capable de maintenir 2 millions de connections TCP
- Capable de soutenir un trafic de 2.6 Gbits/sec
- Statistiques temps réel



SmartBits



2500 



Analyze | ***Assure*** | ***Accelerate***

***MERCI DE VOTRE
ATTENTION***



Analyze | Assure | Accelerate™

April 28, 2005



DES QUESTIONS ?

MERCI DE CONTACTER

Antoine GAUTIER

Ingénieur Technico-Commercial

Tél : 06 85 31 04 38