RealSentry™ SSL overview

AXILIANCE
Internet Security Appliance

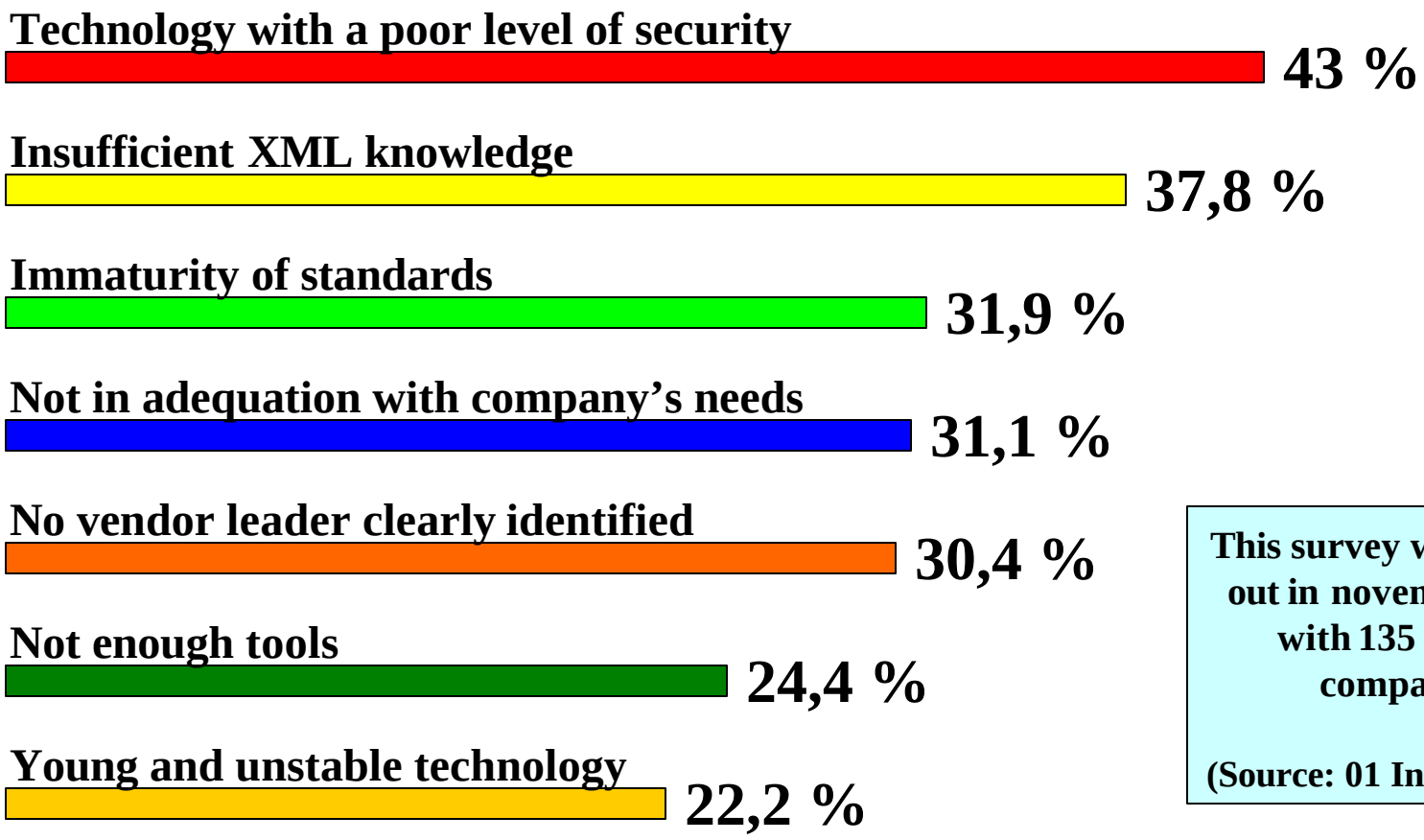
Advanced Protection for Web Services

- ✓ SSL Accelerator
- ✓ Intrusion Detection System
- ✓ Reverse Proxy
- ✓ Application-Firewall

Web services deployment

AXILIANCE
Internet Security Appliance

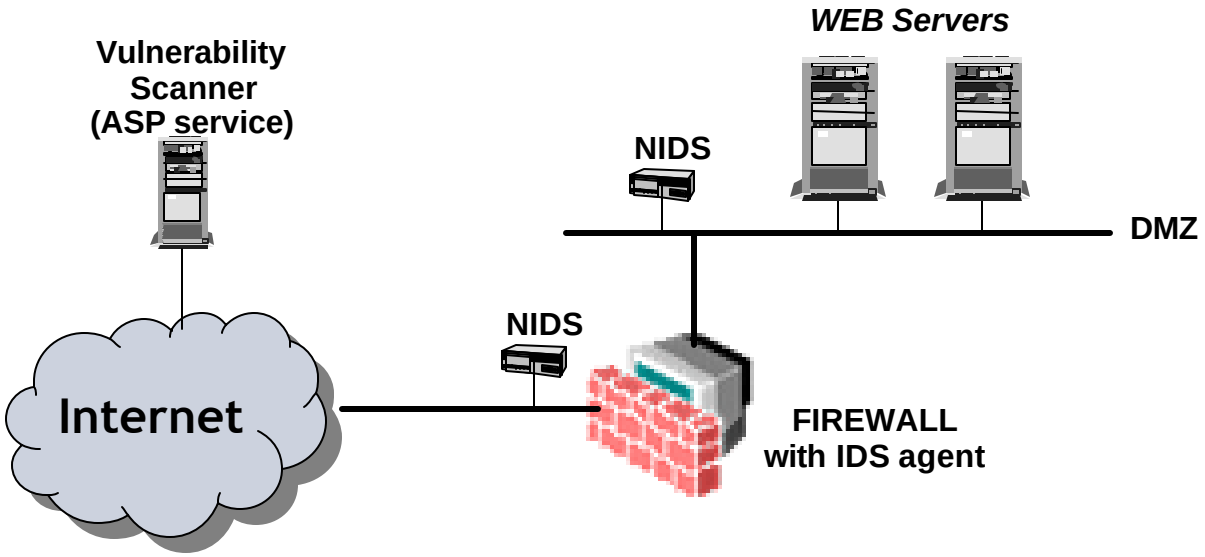
The principal reasons which delay the deployment of web technologies



This survey was carried out in november 2001 with 135 french companies

(Source: 01 Informatique)

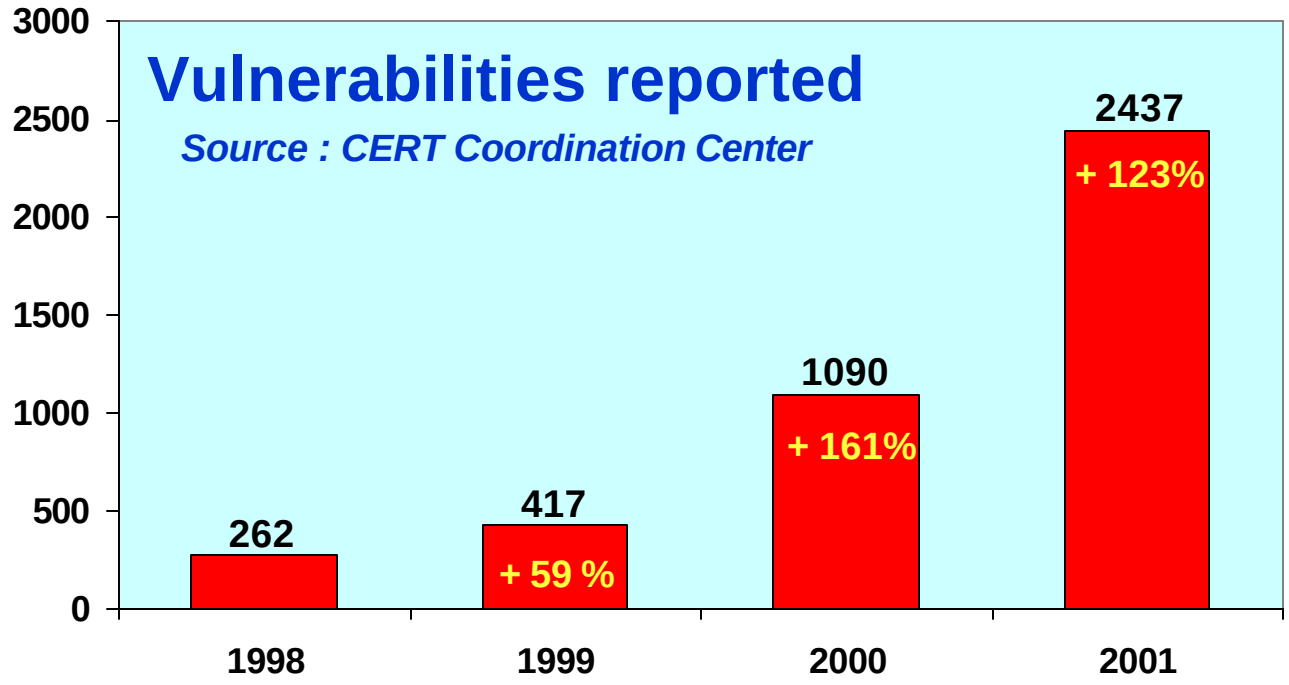
How to protect Web Servers today ?



Today, the best solution uses three components :

- Firewall : To forward only HTTP(S) packets to Web servers
- Network-based Intrusion Detection System (NIDS) : To prevent from malicious packets
- Vulnerability scanner : To detect known vulnerabilities on systems

Vulnerabilities : A worrying progression



Code Red : 2,6 billion US dollars of damage
Nimda : 590 million US dollars of damage

Why are Firewalls insufficient ?

AXILIANCE
Internet Security Appliance

- Security Policy based only on type of protocols (not on content)
- Unable to analyse encrypted network traffic like HTTPS
- Unable to process a finer-grained analysis of the application activities
- Usually protects only from external network
- Network device managed by a security administrator (in opposition with a Web server managed by a webmaster)

Why are NIDS insufficient ?

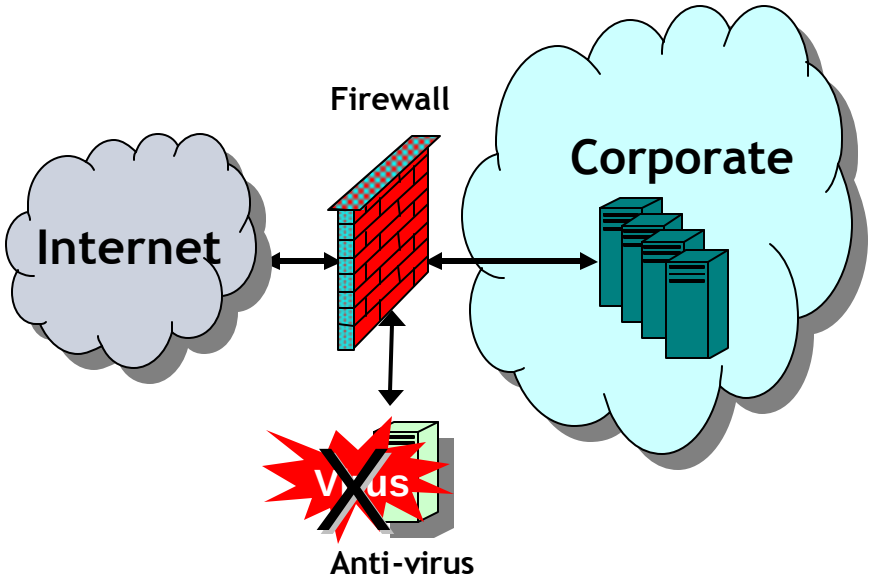
AXILIANCE
Internet Security Appliance

- Protect only against known vulnerabilities (pattern matching)
- Cannot scan content if network traffic is encrypted
- Difficult to deploy on switched networks
- Cannot handle high-speed networks
- Critical setup : Bad configuration generates many false alarms
- Unable to process a finer-grained analysis of the application activities

A new approach against HTTP attacks

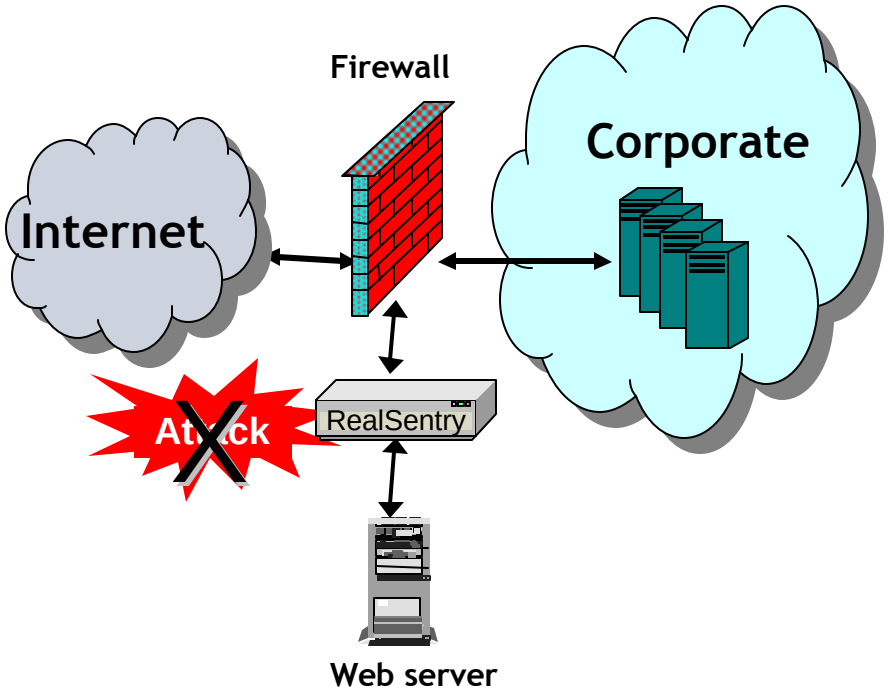
AXILIANCE
Internet Security Appliance

Real-time virus detection



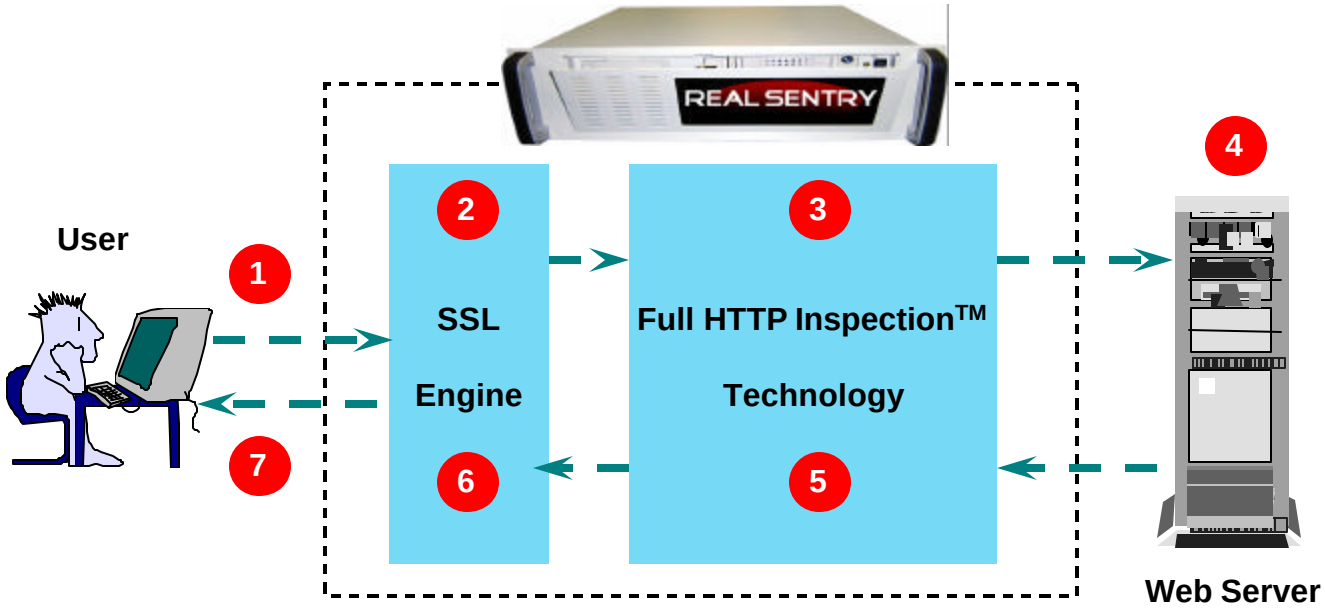
The Antivirus detects and blocks viruses

Real-time HTTP traffic control



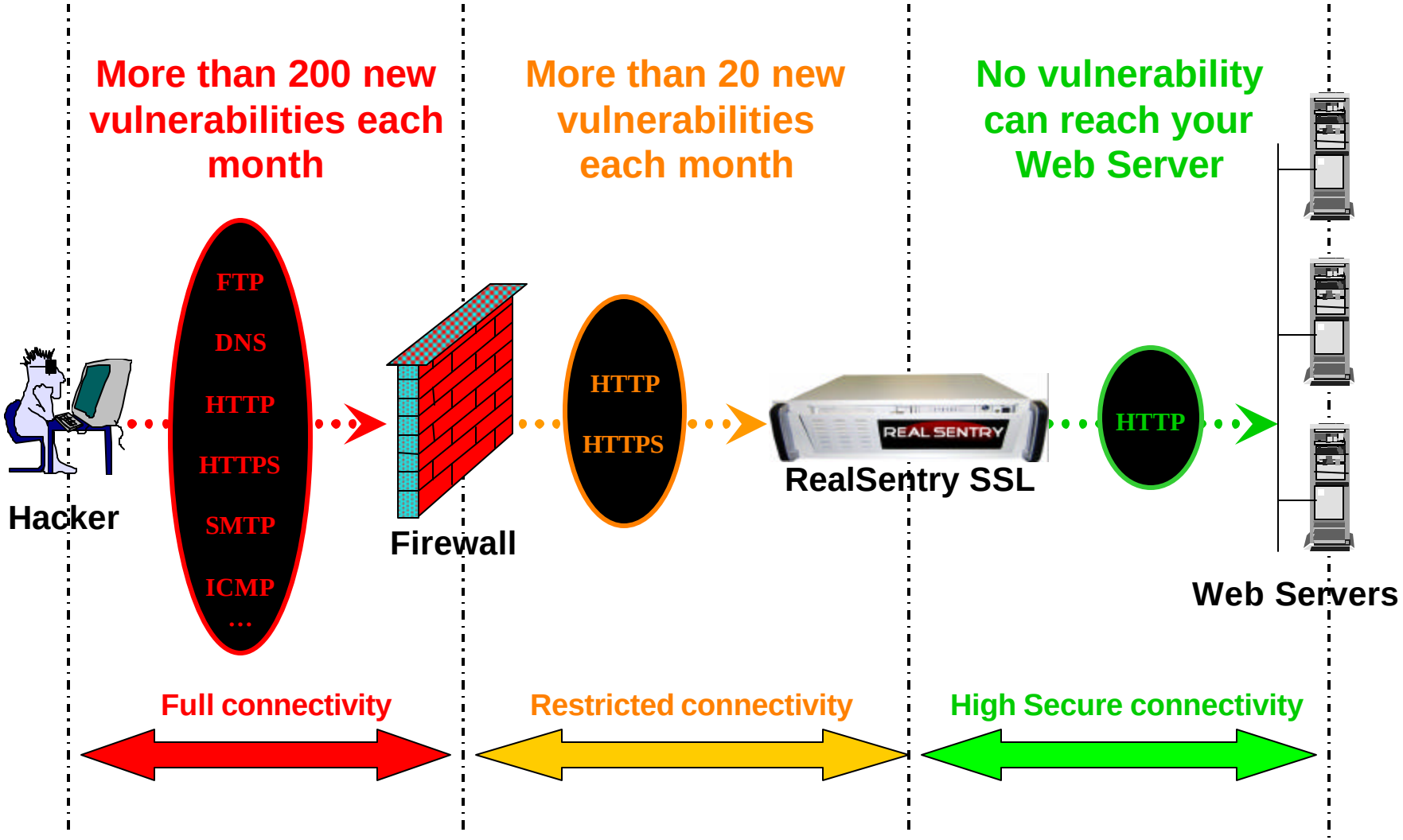
RealSentry detects and protects against known or unknown vulnerabilities

RealSentry concept



(1) HTTP request send by a user
(2) Hardware (RealSentry SSL) or software (RealSentry) decryption
(3) Check HTTP packet with Full Http Inspection^{tm} Technology
(4) If validated by security policy, safe HTTP packet is forwarded to Web Server
(5) Check HTTP packet with Full Http Inspection^{tm} Technology
(6) Hardware (RealSentry SSL) or software (RealSentry) encryption
(7) HTTP answer is sent back to the user

RealSentry provides the ultimate protection



Four technologies in a single box

AXILIANCE
Internet Security Appliance

Reverse Proxy

Like reverse Proxy :

• RealSentry breaks direct connection between browser and Web server.

But unlike Reverse Proxy :

• RealSentry includes filter capabilty to exclude malicious HTTP packets.

• RealSentry keeps original IP address when operates in stealth mode.

NIDS

Like IDS Probe :

• RealSentry is a network-based protection and runs in stealth mode.

But unlike IDS Probe :

• RealSentry protects against unknown vulnerabilities.

• RealSentry protection is effective even on encrypted packets (HTTPS).

Application Firewall

Like Application Firewall :

• RealSentry allows to implement a security Policy to accept or deny packets.

But unlike Application Firewall :

• RealSentry performs a detailed protocol analysis to prevent against malicious HTTP requests.

SSL Accelerator

Like SSL Accelerator :

• RealSentry handles decryption and encryption tasks for SSL transactions.

But unlike SSL Accelerator :

• RealSentry incorporates built-in security mechanism to protect your web site from fraudulent activities.

RealSentry Technology

Black List Detection (IDS technology)

- **Concept**
  - Signature-based method
  - Requires regular updates
  - Protects only against known vulnerabilities

- **RealSentry Implementation**
  - Automatic updates
  - Multiple rules to prevent IDS evasion
  - Very easy to setup : Protect your Web server in a few minutes

- **RealSentry Benefits**
  - Detects more than 600 HTTP vulnerabilities
  - Effective protection including on encrypted traffic (HTTPS)
  - No need to monitor vulnerabilities or patch your Web server
  - Plug and Protect solution

RealSentry Technology

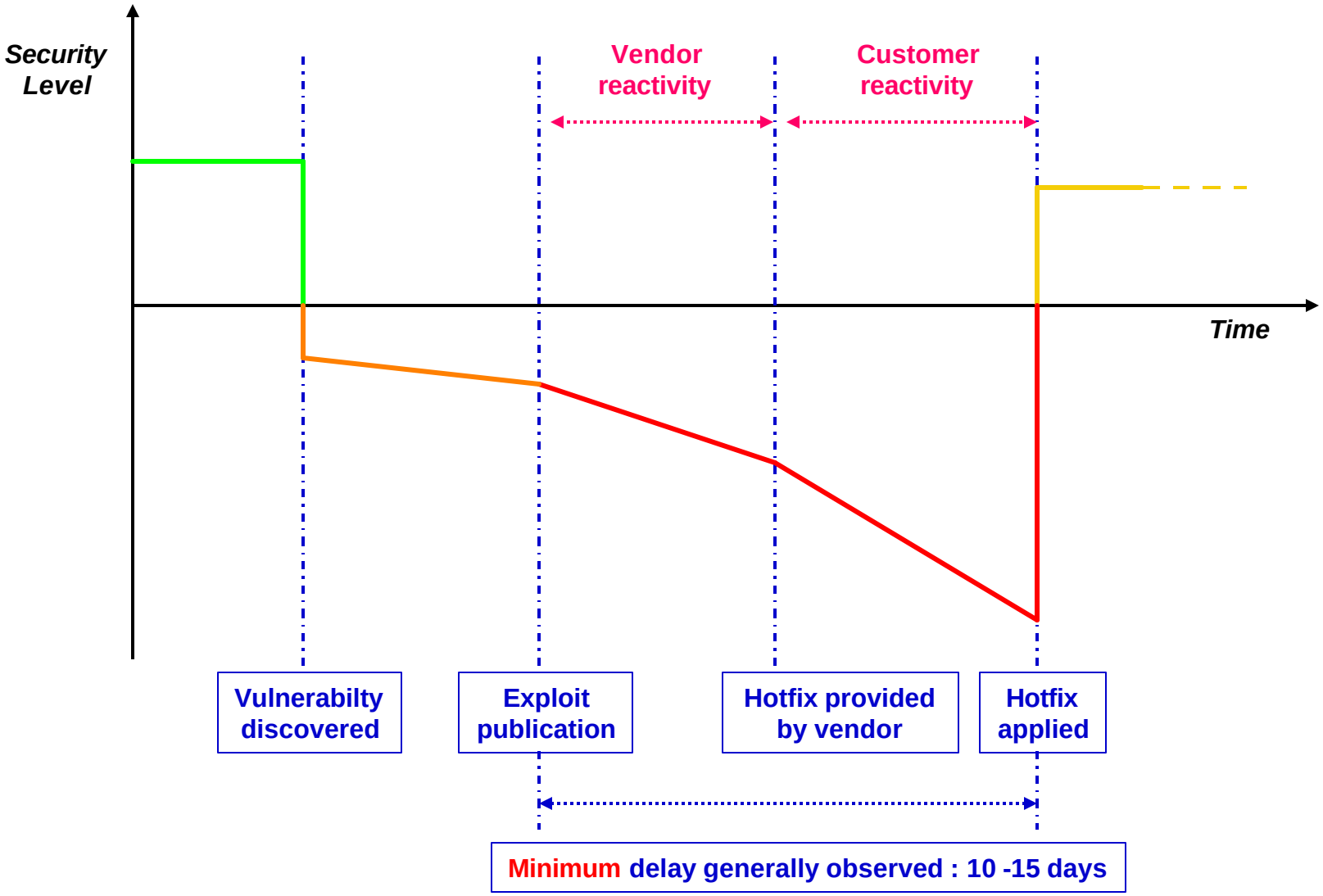
White List Filtering (Exclusive Axiliance technology)

- **Concept**
  - All HTTP requests that are not expressly authorized are prohibited
  - Non signature-based method
  - Protection against known or unknown vulnerabilities

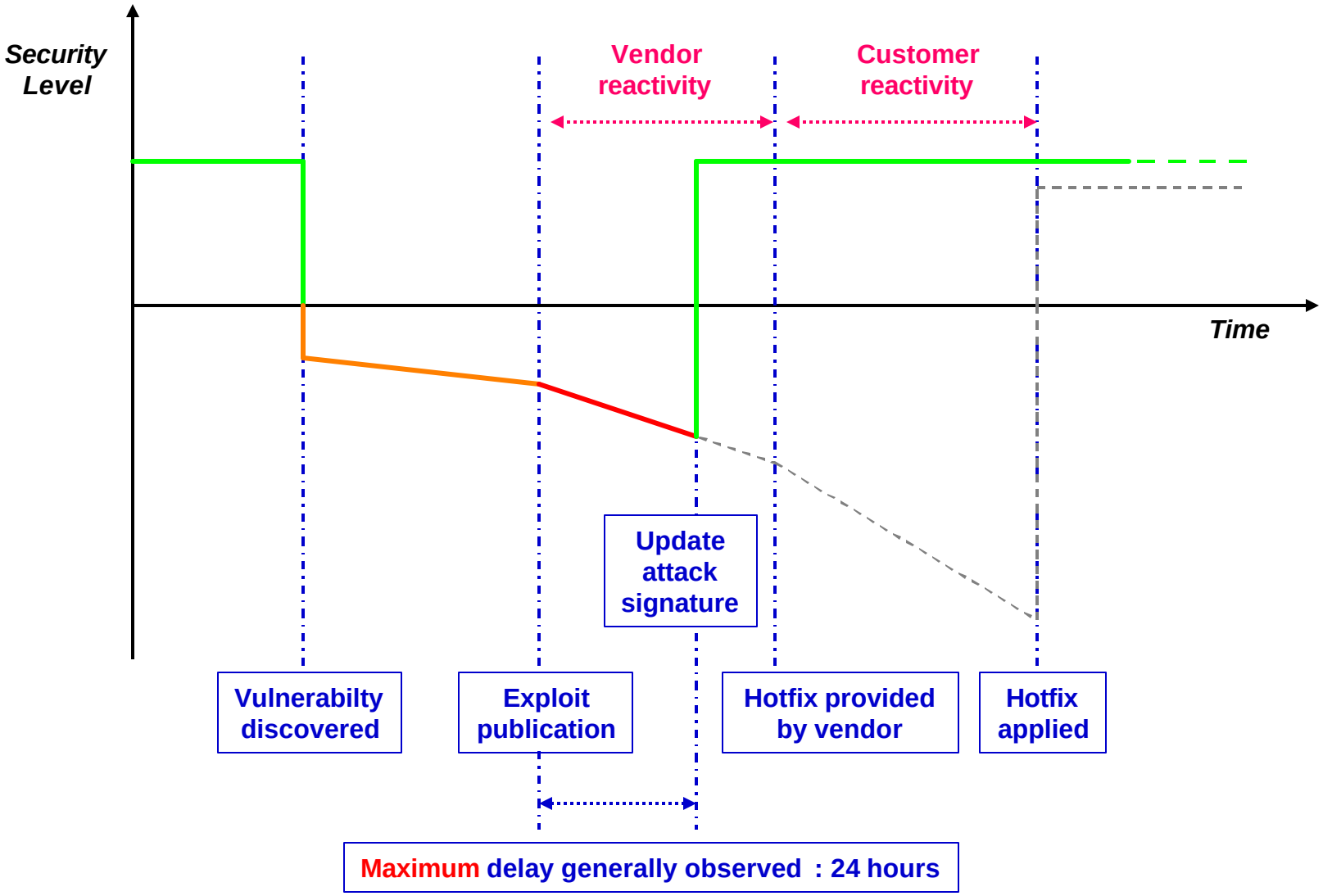
- **RealSentry Implementation**
  - Security Policy define by URL groups, directories or single URL
  - Security Policy includes syntax, URL length, Variables, cookies, …
  - Setup assistants with learning, tracking and protecting modes

- **RealSentry Benefits**
  - Identify and prevent both known and unknown vulnerabilities
  - Effective protection including on encrypted traffic (HTTPS)
  - Represents the most secure solution for Web services currently available in the world

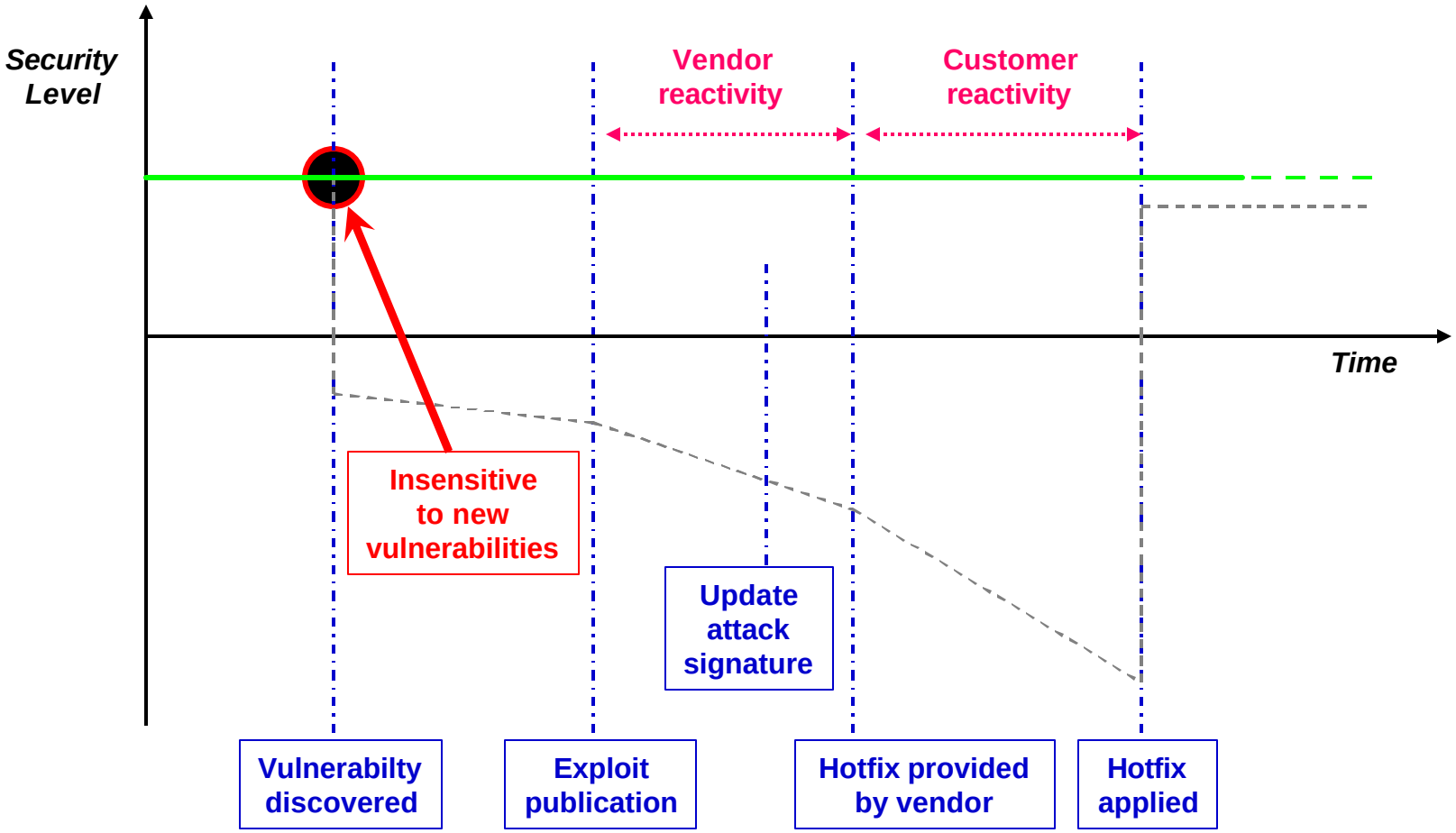
Normal Life Cycle of a vulnerability …



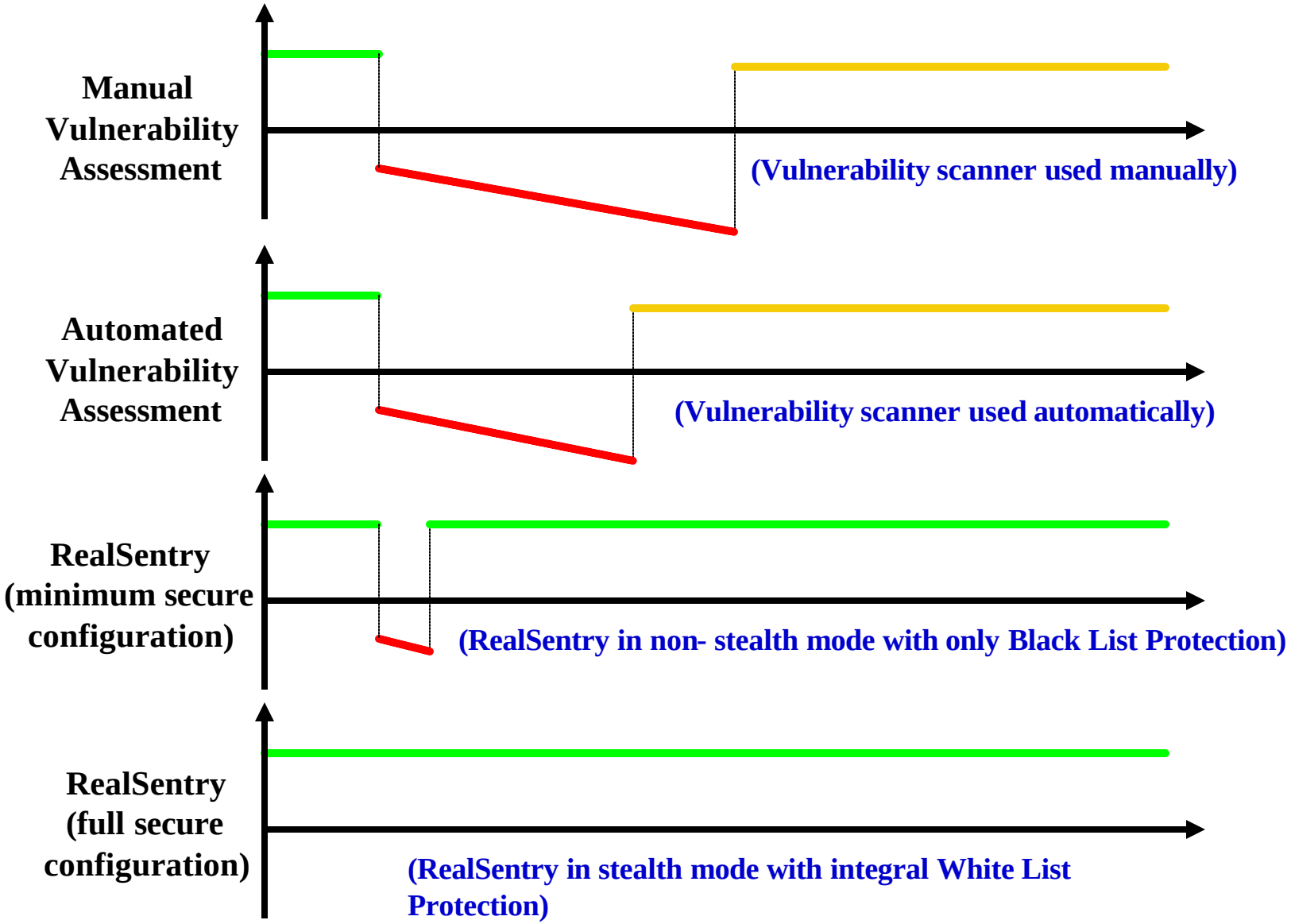
RealSentry with only Black List Protection



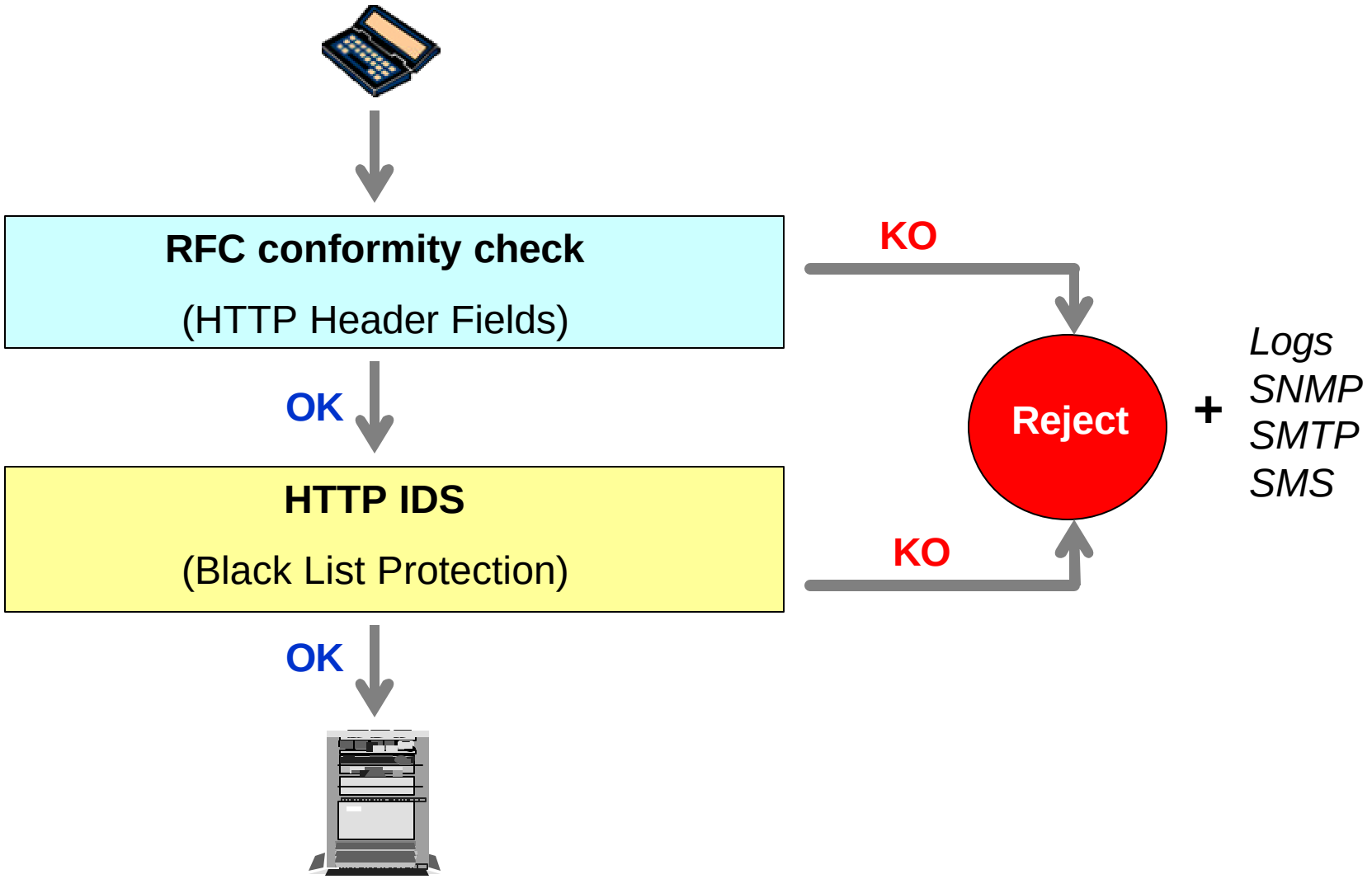
RealSentry with White List Protection



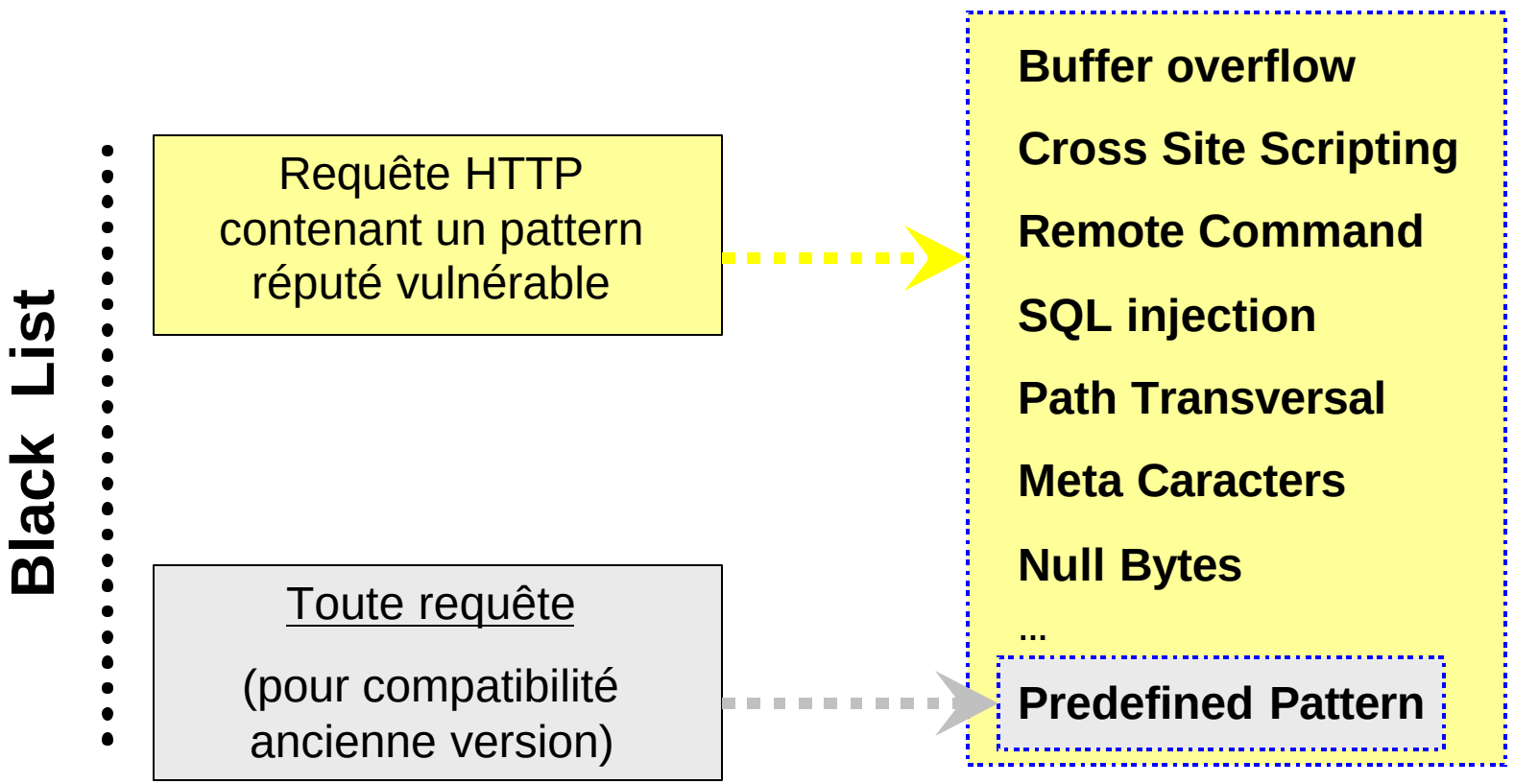
The 4 solutions to prevent vulnerabilities



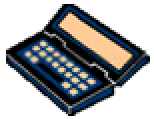
Black List Mode



Counter measures with HTTP IDS



White List + Black List



Client

RFC conformity check

HTTP Headers Management

KO

OK

OK

OK

HTTP Firewall

(Partial White List)

HTTP Firewall

(Full White List)

KO

Reject

+

Alerts

Logs
SNMP
SMTP
SMS

OK

OK

OK

HTTP IDS

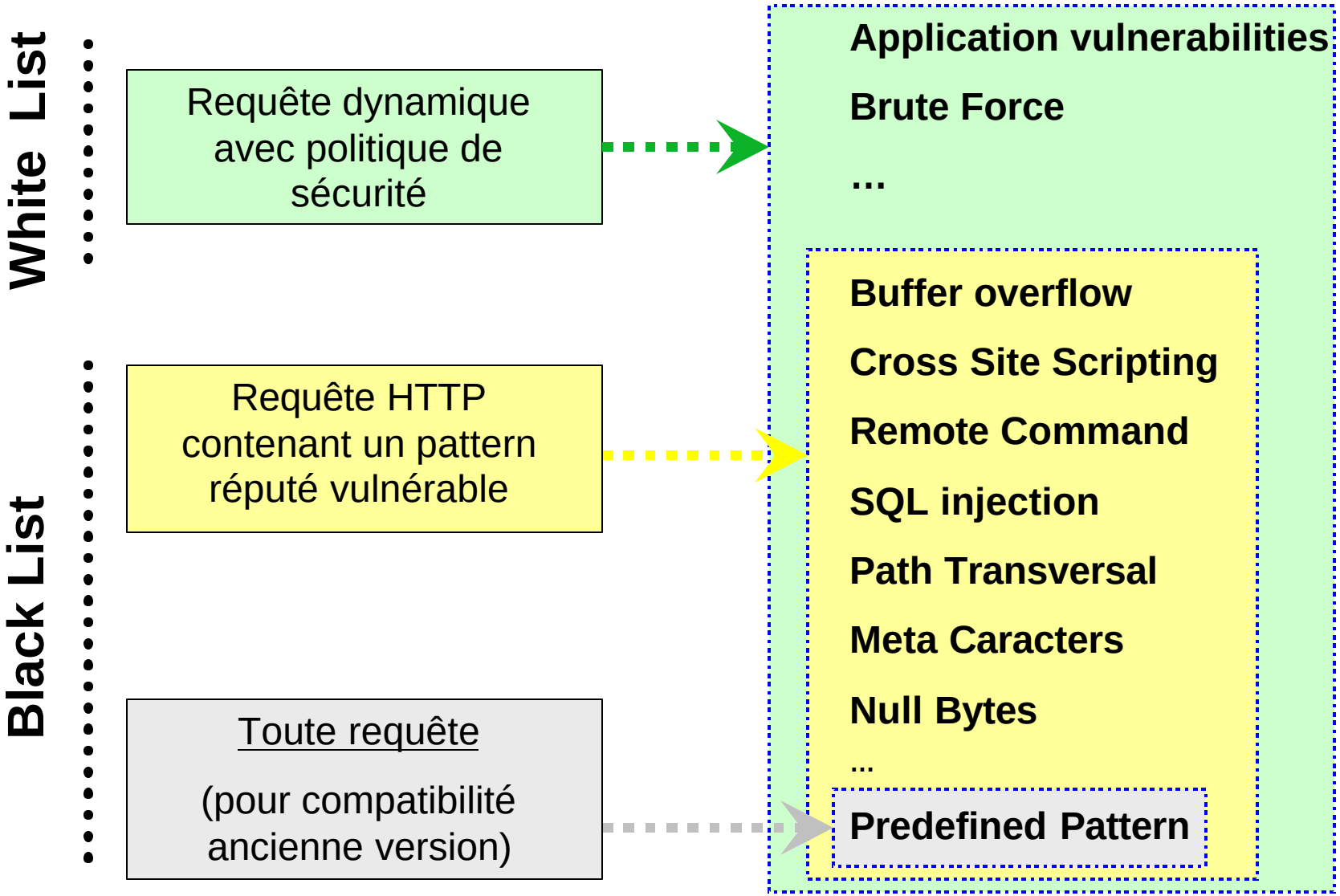
(Black List Protection)

KO

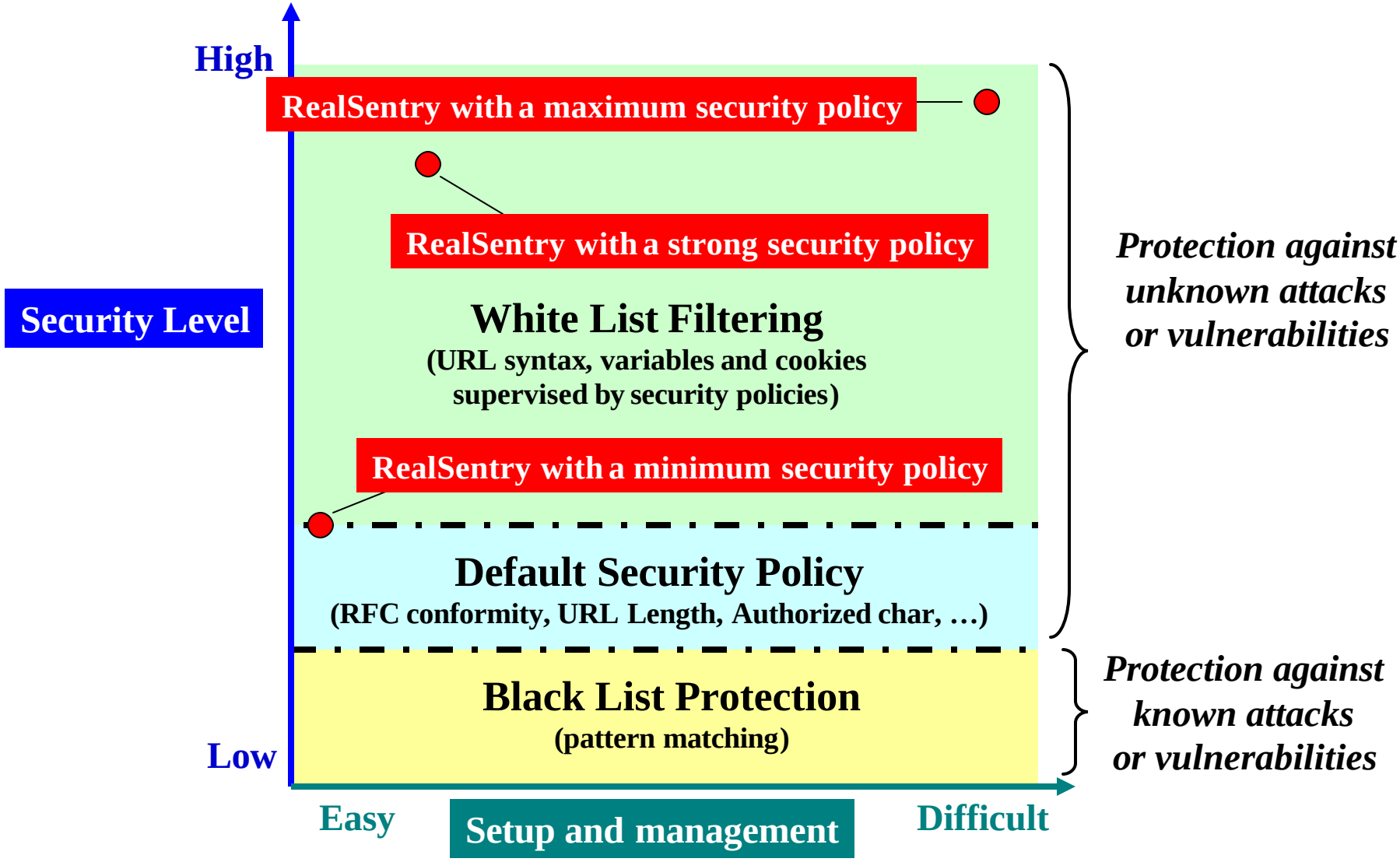
OK

Web Server

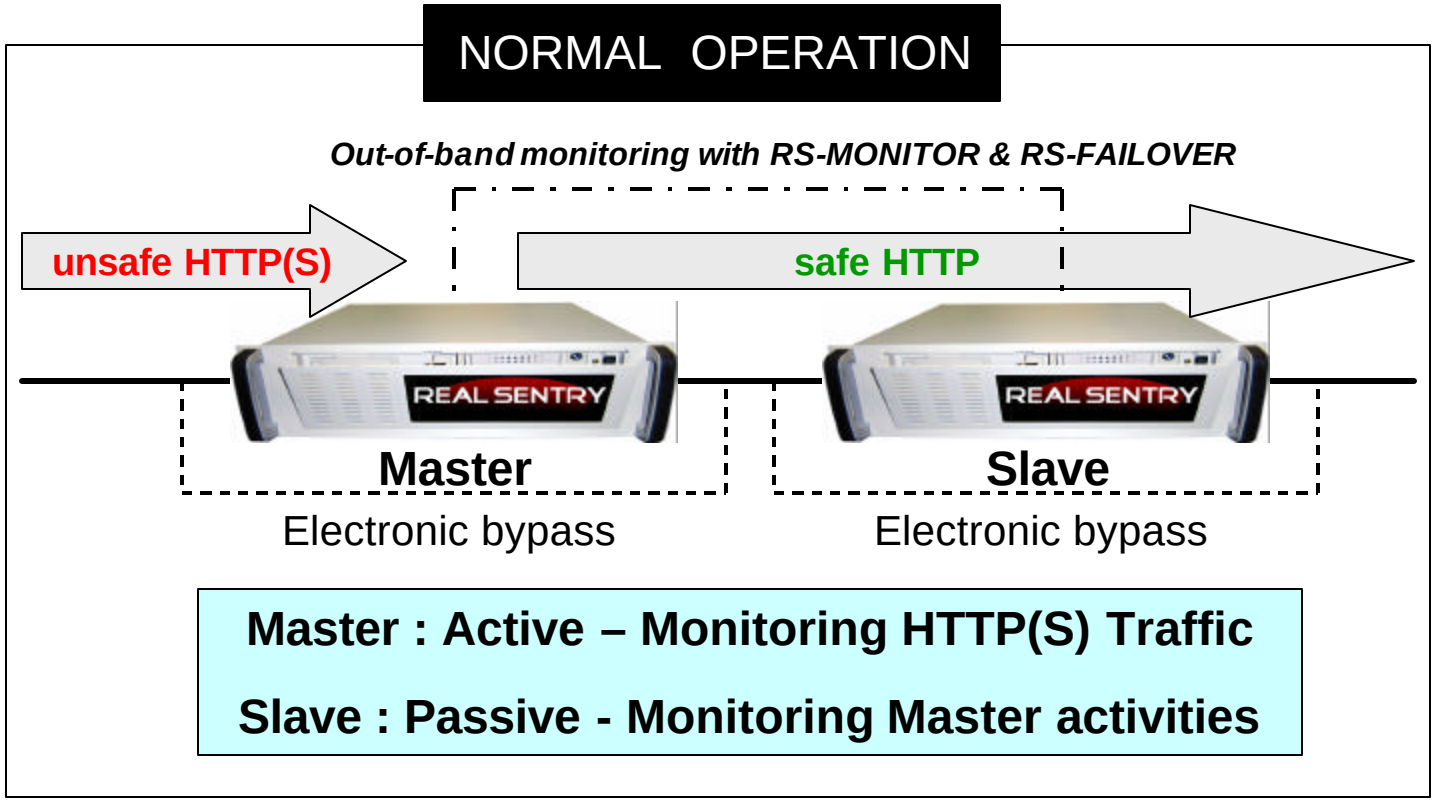
Counter measures with IDS et FW HTTP



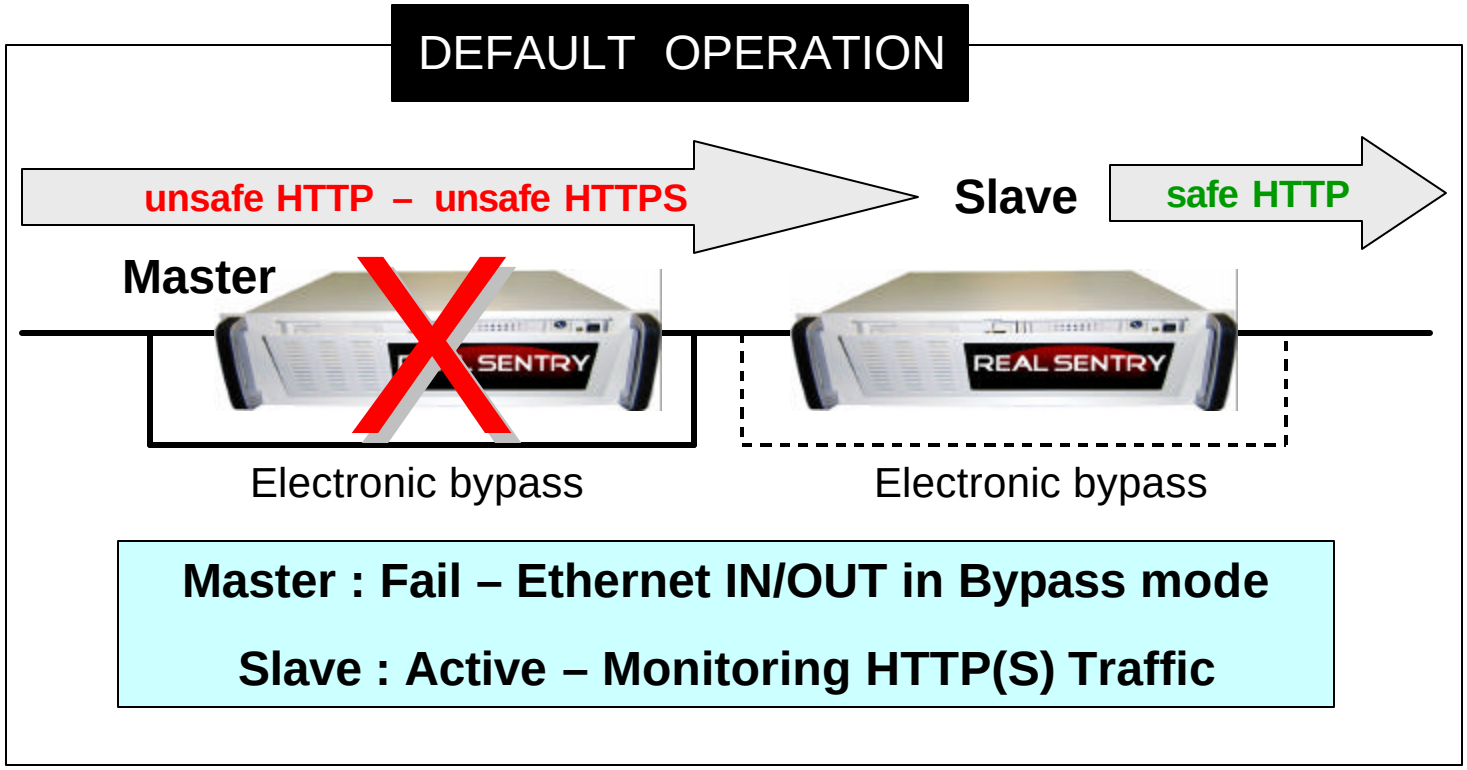
RealSentry Security Level



High Availability : Normal operation



High Availability : Fault operation



RealSentry SSL v1.0 Features

AXILIANCE
Internet Security Appliance

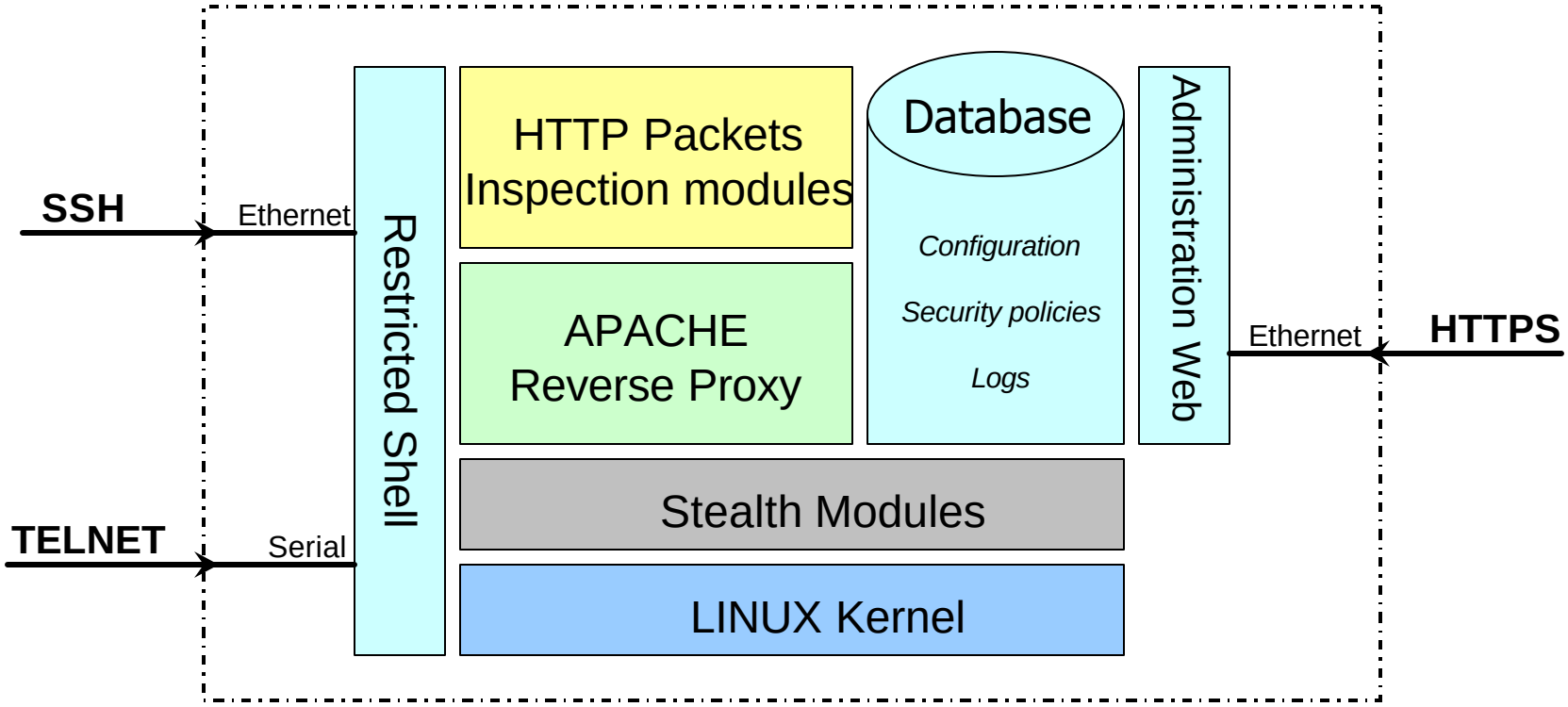
APPLIANCE	Integrated solution (hard and soft)
SSL ACCELERATION	Boosted and secure encrypted traffic
INTRUSION DETECTION	Exclusive technology from Axiliance
STEALTH MODE	« Plug and Protect » solution
FAULT TOLERANCE	High availability - 24/7

Competitive Comparisons

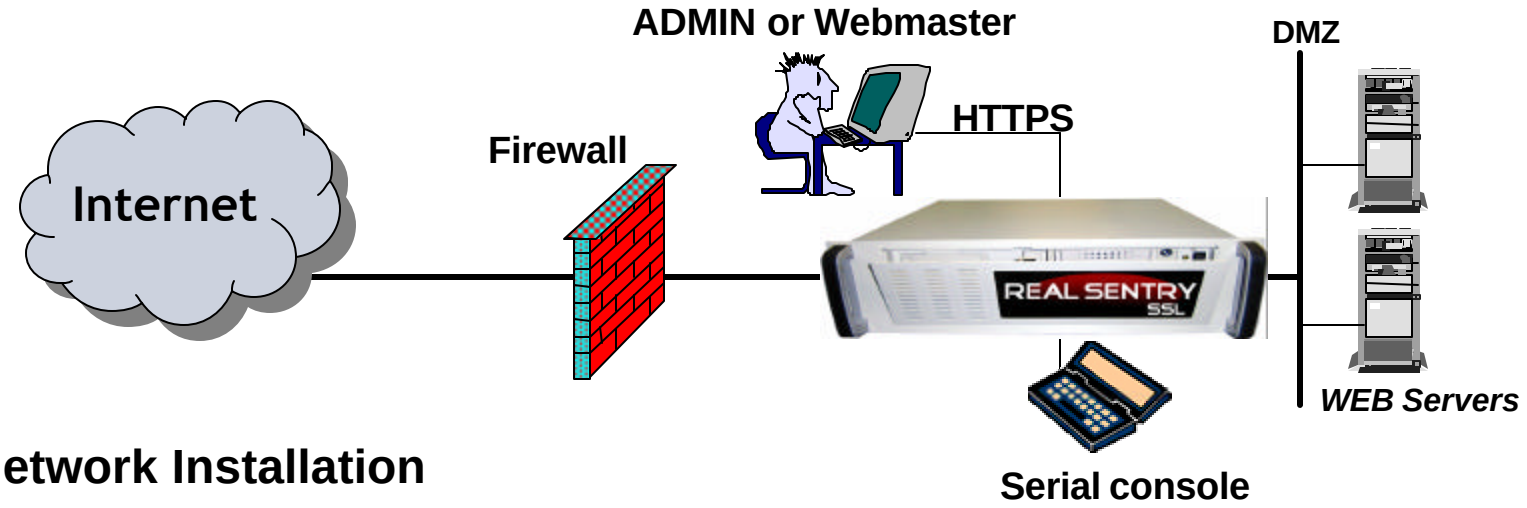
Company	Product	Native Fault Tolerance	Stealth Mode	SSL Acceleration	Appliance
Kavado	Interdo	No	No	Yes	Yes
Sanctum Inc	AppShield	No	Yes	compliant with 3rd party	Option
Deny-All	Rweb	No	No	compliant with 3rd party	No
Ubizen	dmz/shield	No	No	compliant with 3rd party	Option
Stratum 8	APS	No	No	No	Yes
Axiliance	RealSentry	Yes	Yes	No	Yes
Axiliance	RealSentry SSL	Yes	Yes	Yes	Yes

RealSentry : Setup and management

Full out-of-band management by
serial or ethernet interface



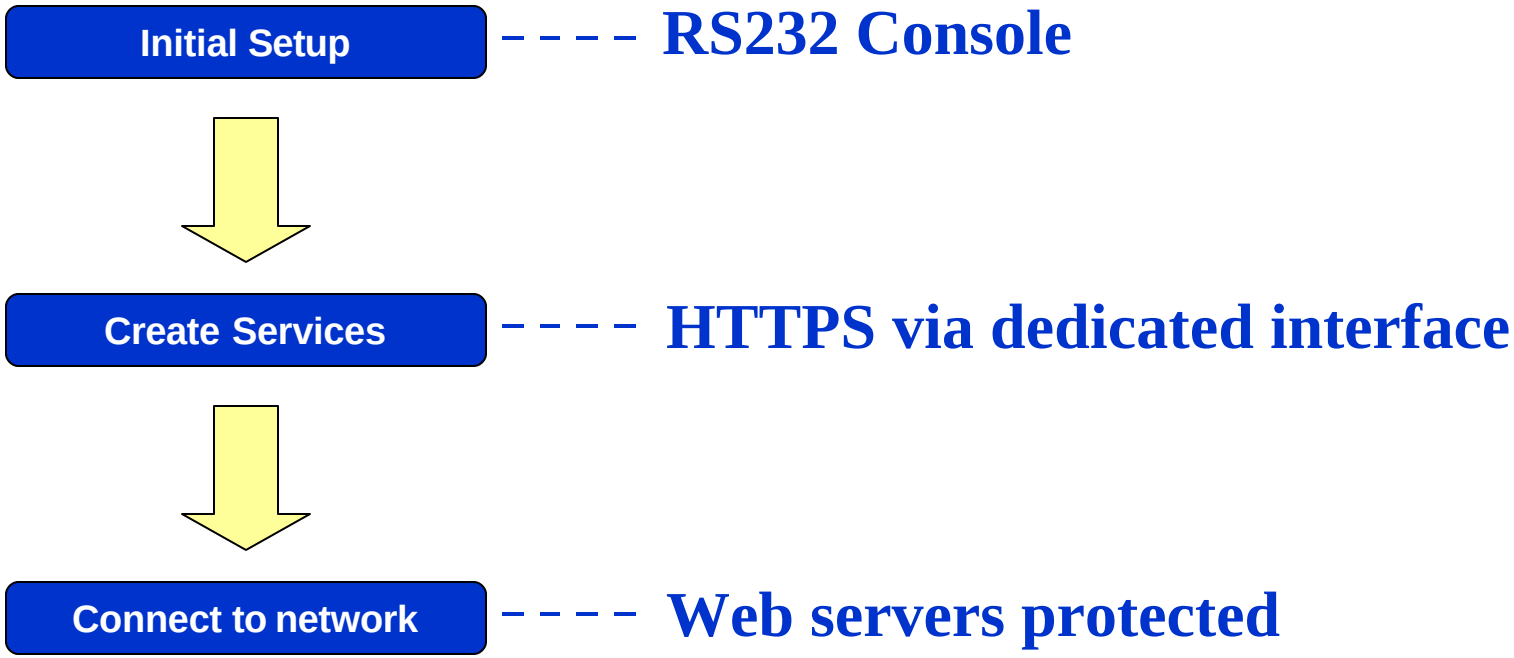
RealSentry : Setup and management



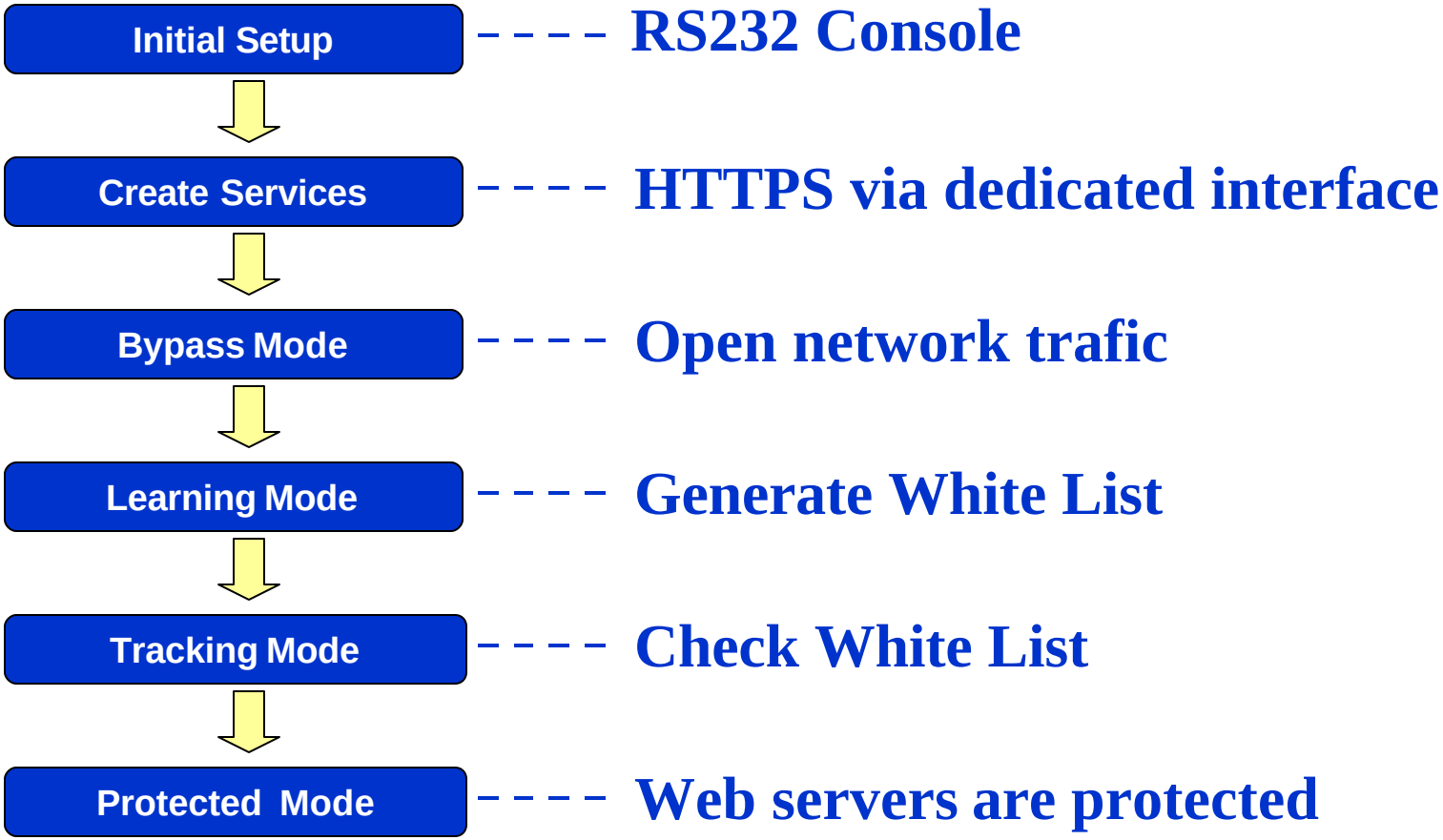
- **Network Installation**
  - First setup by serial console
  - Access restricted to a special account (ADMIN)

- **Management of services and security policies**
  - Network Interface card dedicated to management operations
  - Intuitive and secure Web-based administration (HTTPS)
  - Command line based administration via restricted and secure shell
  - Service creation is only allowed to an administrator account (ADMIN)
  - Each service is associated to one or several Webmaster
  - Services Management is only allowed to the Webmaster

Black List Mode



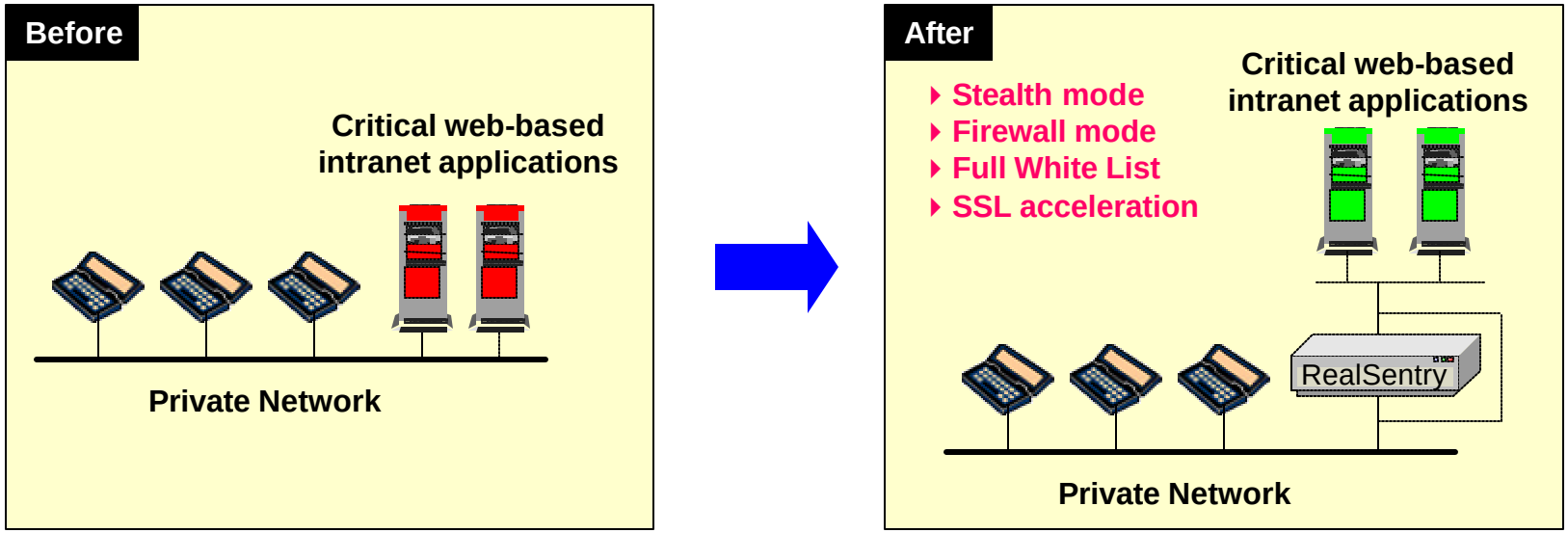
White List Mode



Case Studies

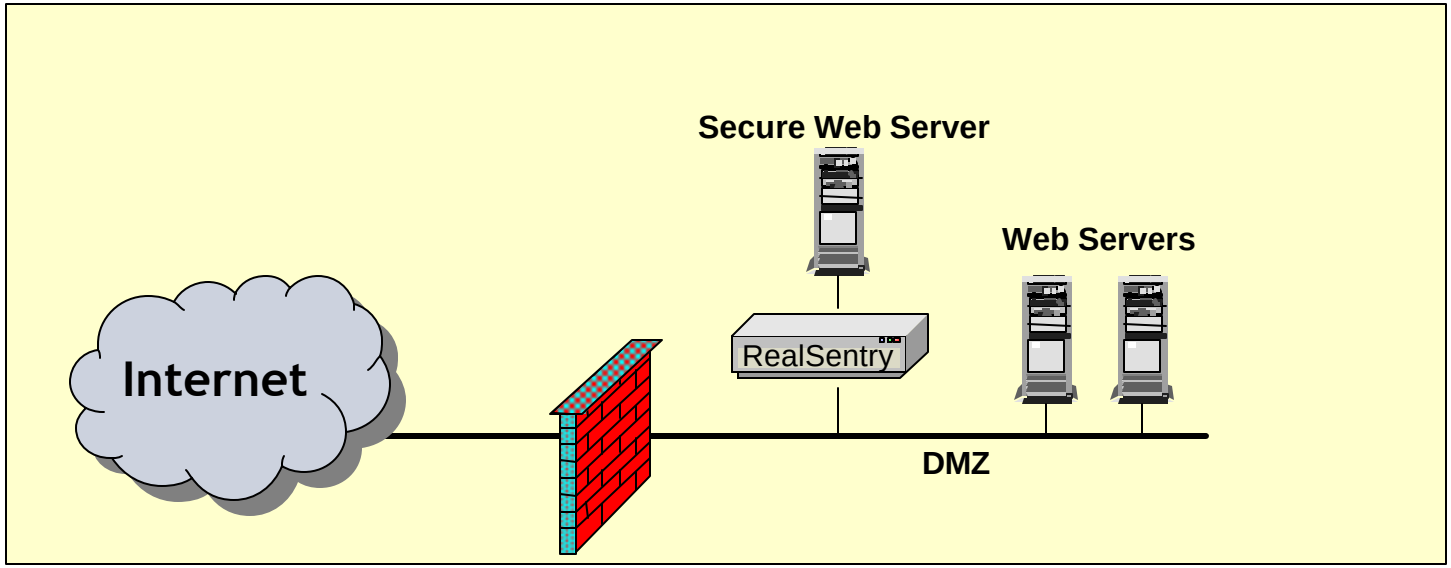
- Case Study 1 : RealSentry SSL protects Intranet Web Servers
- Case Study 2 : RealSentry dedicated for hosting in ISP architecture
- Case Study 3 : RealSentry mutualized for hosting in ISP architecture
- Case Study 4 : DMZ Protection with non transparent mode
- Case Study 5 : DMZ Protection with stealth mode
- Case Study 6 : Multiple DMZ Protection with non transparent mode
- Case Study 7 : Multiple DMZ Protection with stealth mode

CS1 : Intranet Web Servers Protection

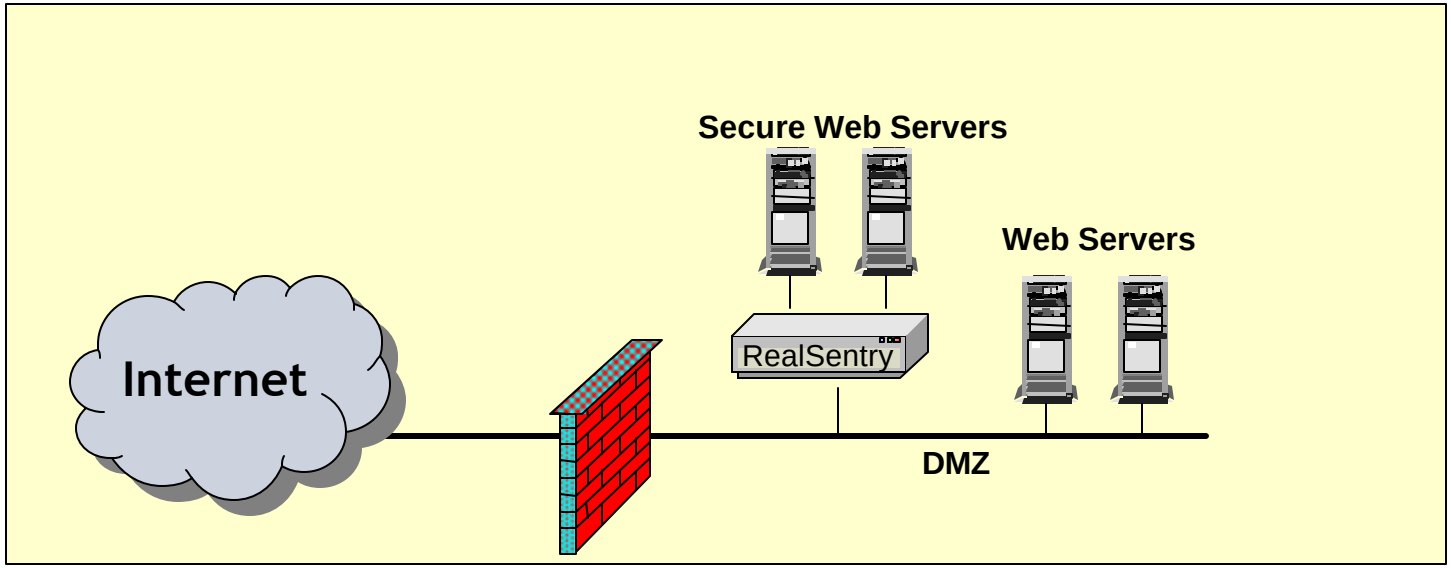


- **Customer benefits :**
  - Forward only HTTP(S) packets to Web Server (Firewall mode)
  - Protect Web server against known or unknown HTTP Attacks
  - Non restrictive SSL usage without need to upgrade server hardware
  - Installation without any network modification
  - Native simple fault tolerance by electronic bypass

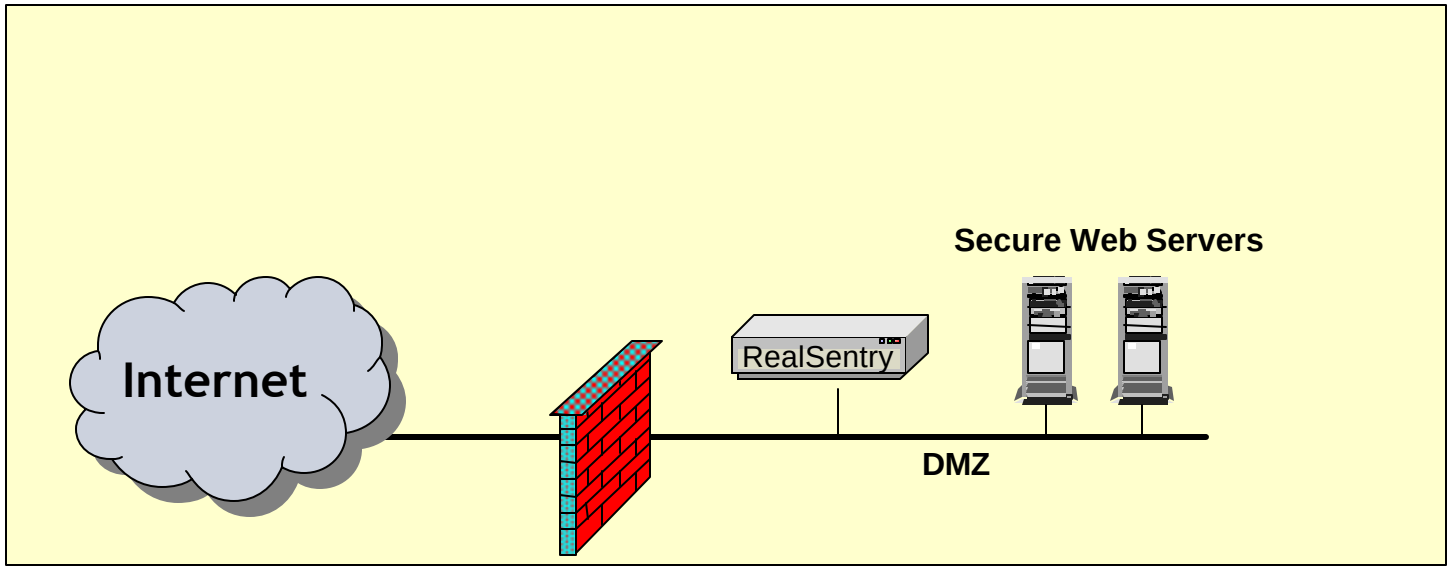
CS2 : RealSentry dedicated for ISP



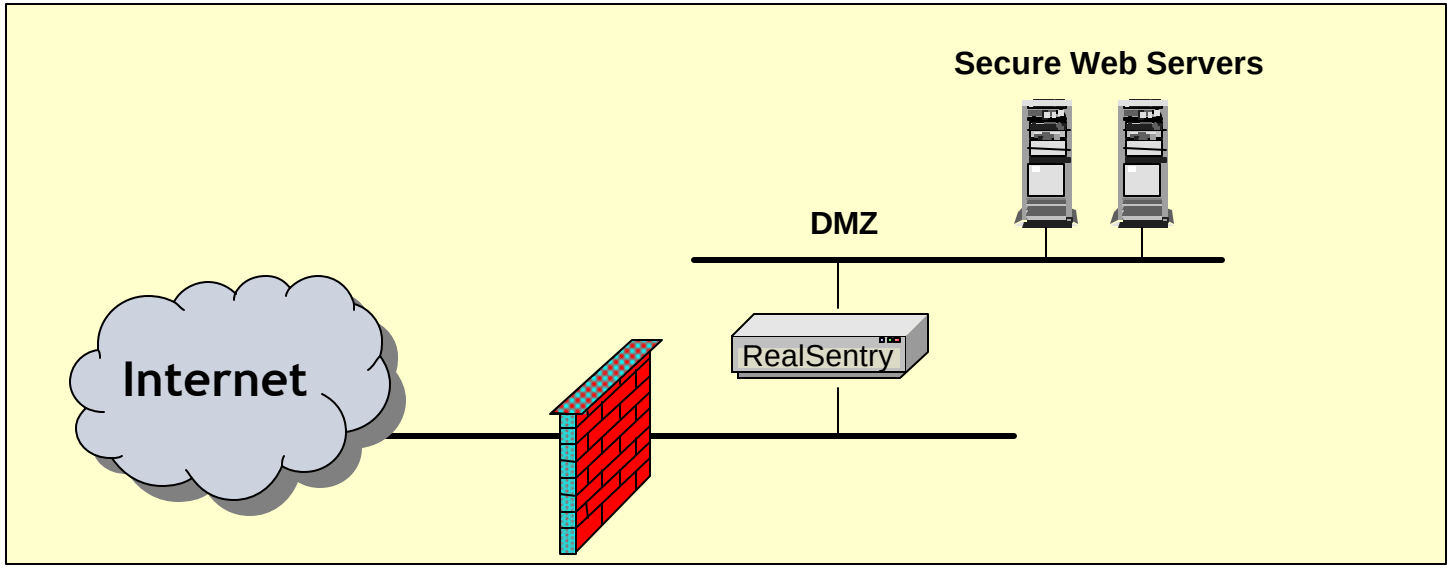
CS3 : RealSentry mutualized for ISP



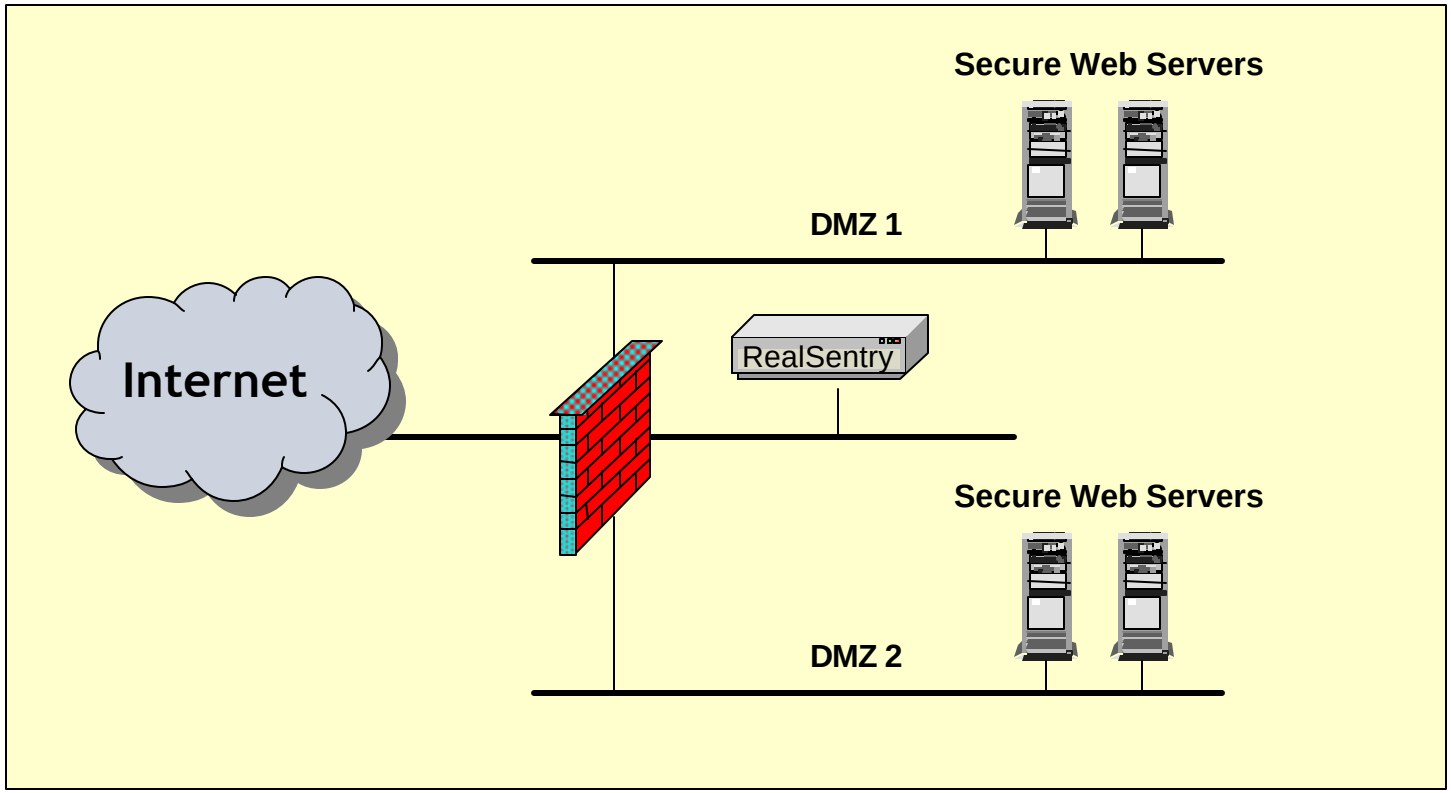
CS4 : Non Transparent Mode



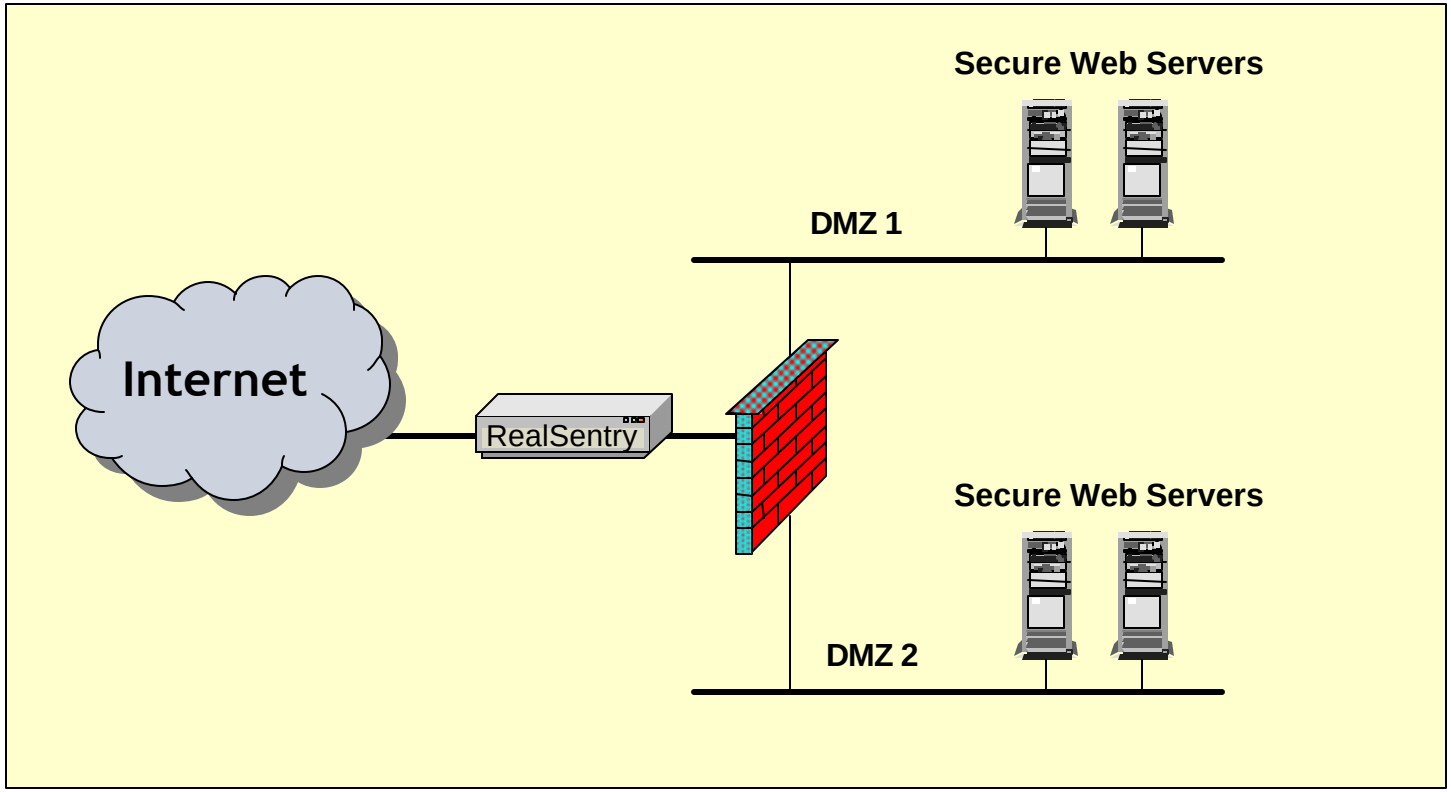
CS5 : Stealth Mode



CS6 : Multiple DMZs – Non Transparent



CS7 : Multiple DMZs – Stealth Mode



Thank you for your attention

Boris MOTYLEWSKI

e-mail : bm@axiliance.com

AXILIANCE S.A.
Société Anonyme au capital de 120 000 Euros
Siège social : Montpellier - FRANCE

TEL : +33 (0)4 67 79 79 31
FAX : +33 (0)4 67 79 79 32

WEB : http://www.axiliance.com
MAIL : info@axiliance.com