Web Application Firewalls: Panel Discussion

Sebastien Deleersnyder
CISSP
Feb, 2006
sdl@ascure.com

OWASP

Agenda

- Panel Introduction
- WAF Primer
- Panel Discussion

Agenda

- Panel Introduction
- WAF Primer
- Panel Discussion

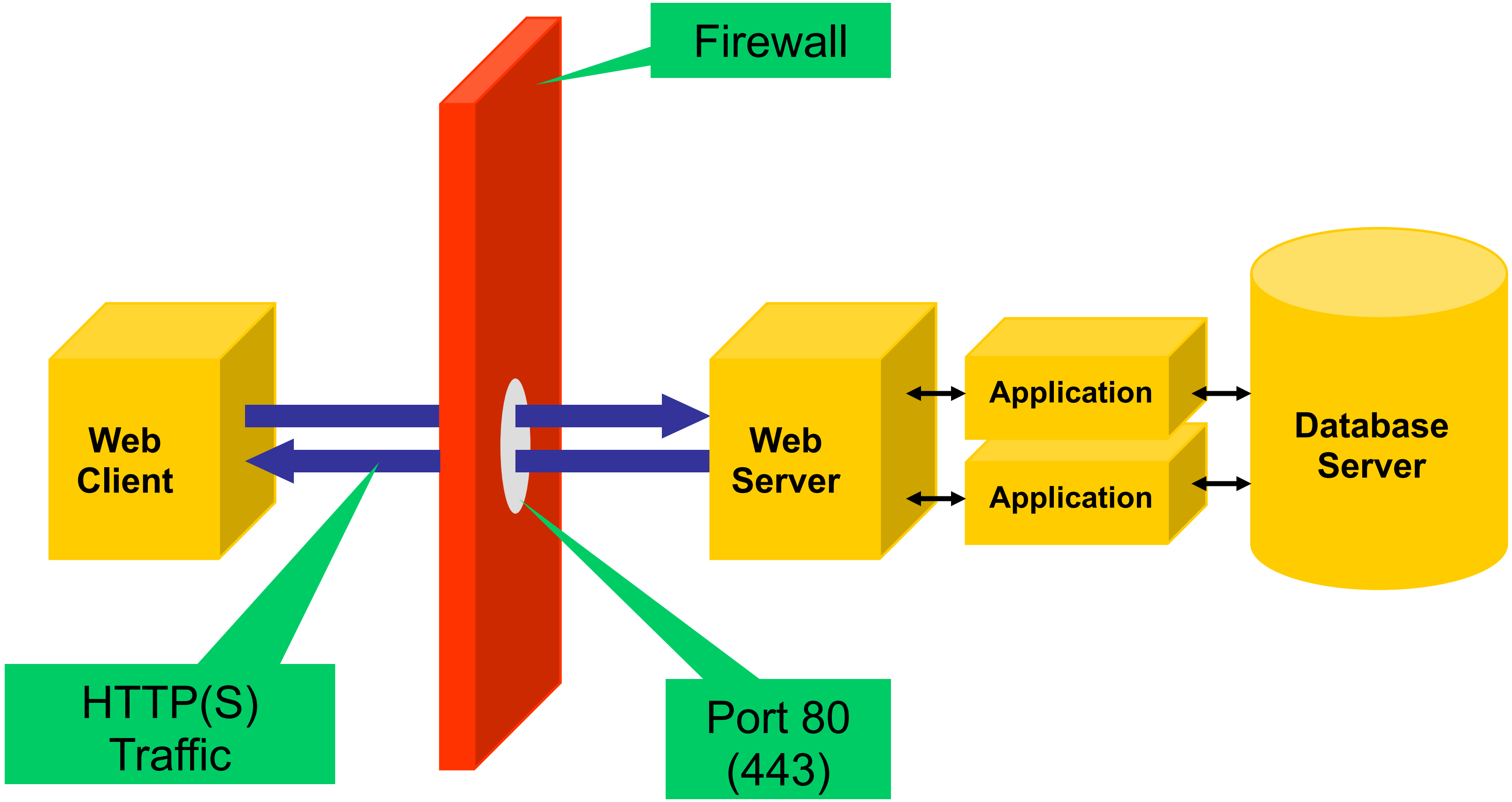
Panel Introduction

- Philippe Bogaerts, BeeWare
- Jaak Cuppens, F5 Networks
- Tim Groenwals, Agfa Gevaert
- Lieven Desmet, K.U.Leuven
- David Van der Linden, ING

Agenda

- Introduction
- WAF Primer
- Panel Discussion

Network Firewalls Do Not Work



Enter Web Application Firewall Era

- HW/SW that mitigates web application vulnerabilities:
  - Invalidated Input
  - Parameter tampering
  - Injection Flaws
  - …

Web Application Firewalls

- They understand HTTP/HTML very well
- They work after traffic is decrypted, or can otherwise terminate SSL
- Prevention is possible

Topologies

- Network-based:
  - Protects any web server
  - Works with many servers at once
- Web server-based:
  - Closer to the application
  - Limited by the web server API

WAF functionality

- Rule-based:
  - Uses rules to look for known vulnerabilities
  - Or rules to look for classes of attack
  - Rely on rule databases
- Anomaly-based:
  - Attempts to figure out what normal operation means

WAF Protection Strategies

- Negative security model:
  - Deny what might be dangerous.
  - Do you always know what is dangerous?
- Positive security model:
  - Allow what is known to be safe.
  - **Positive security model is better.**

Vendors

- MOD-Security
- Beeware IntelliWall
- Citrix NetScaler Application Firewall (Teros)
- DenyAll rWeb
- F5 TrafficShield (Magnifire)
- Imperva SecureSphere
- Netcontinuum
- Breach BreachGate WebDefend
- …
- eEye SecureIIS
- Microsoft URLScan

WAF?

- CheckPoint Application Intelligence?
- MS ISA Server?

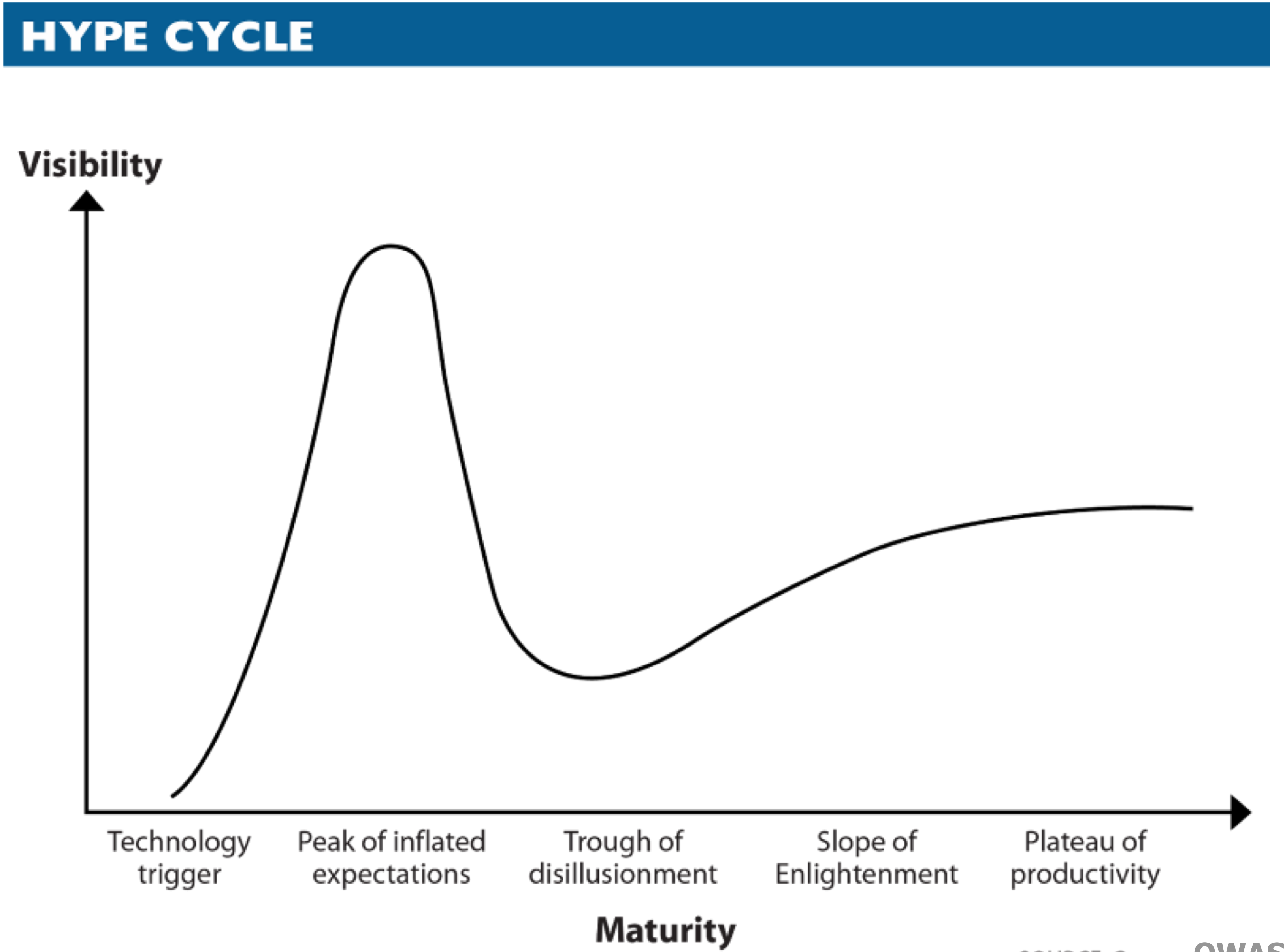
Dead:

- Kavado InterDo
- Watchfire AppShield (Sanctum)
- Ubizen DMZShield

Agenda

- Introduction
- WAF Primer
- Panel Discussion

How mature are WAFs?



SOURCE: Gartner

Panel Discussion

- What do WAFs protect you from? What not?
- Where do you position WAFs in your architecture?
- What WAF functionality do you really need?
- How to reduce TCO?
- Who administrates a WAF within the organisation?