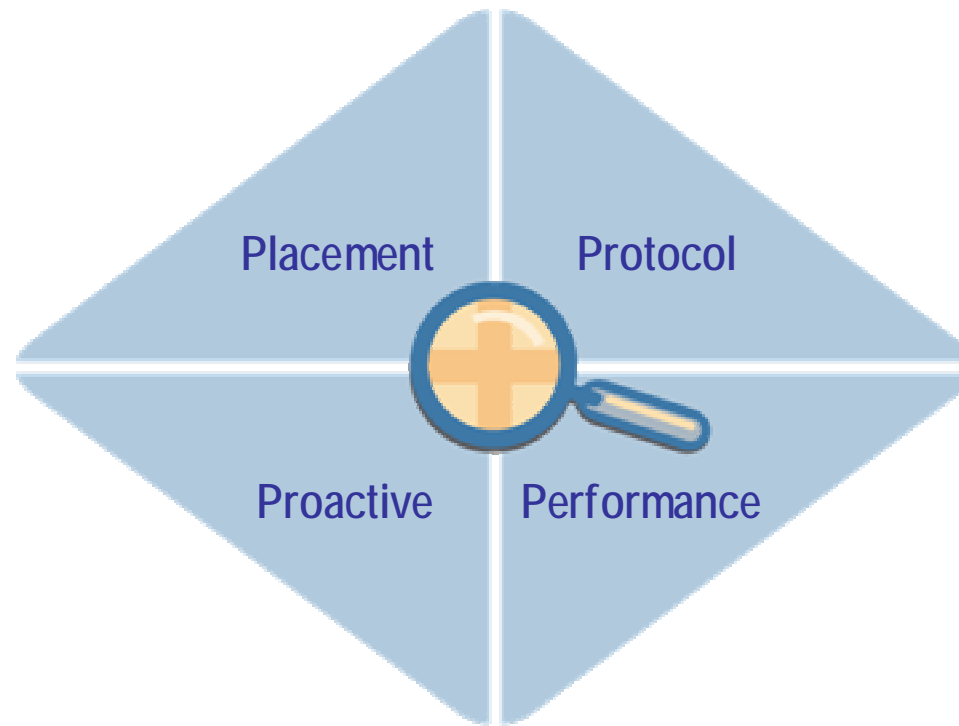




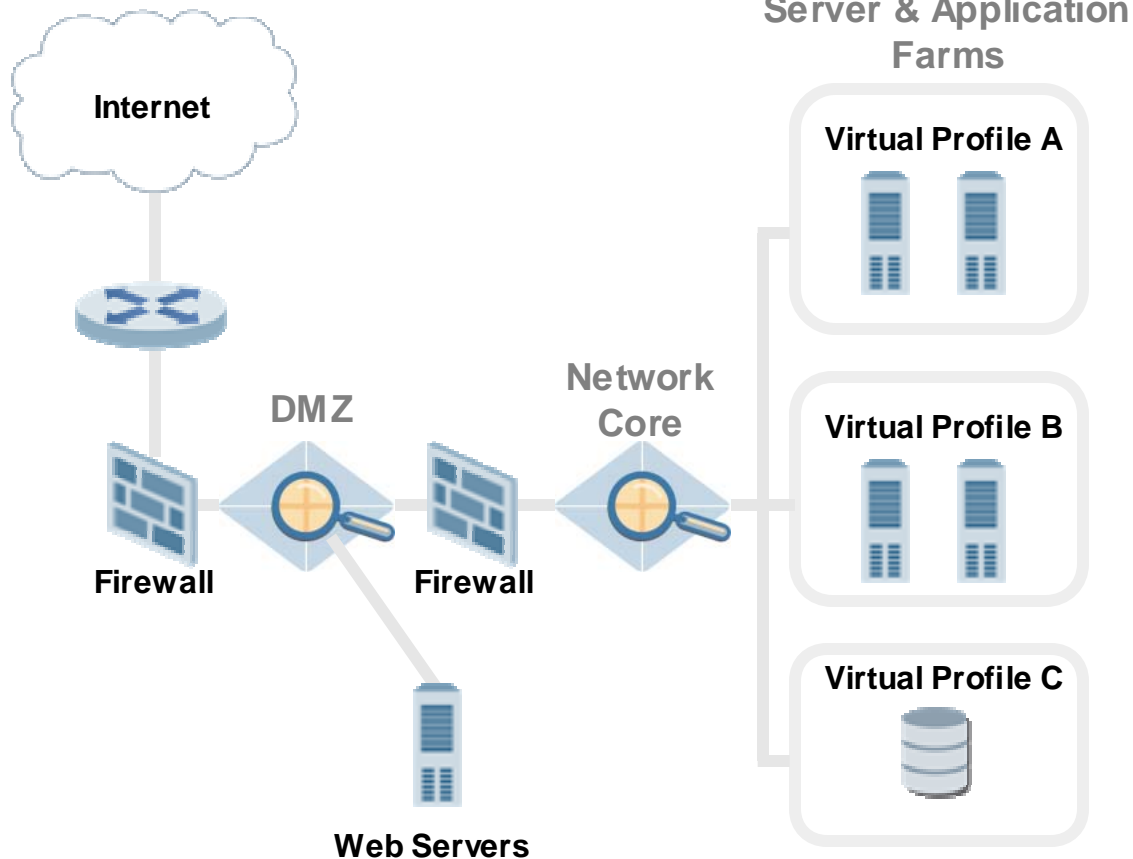
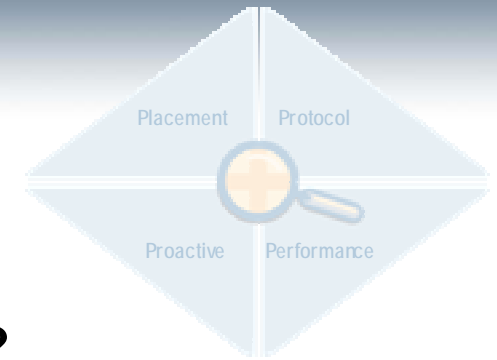
The 4 P's of Application Security



Jeff Pancottine
Senior Vice President • F5 Networks, Inc.
May 13, 2004



Placement



DMZ?

- Only external attacks
- Generic attack protection

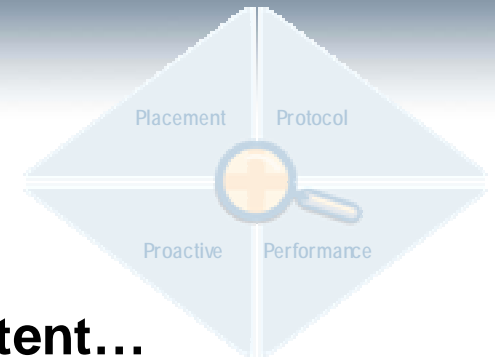
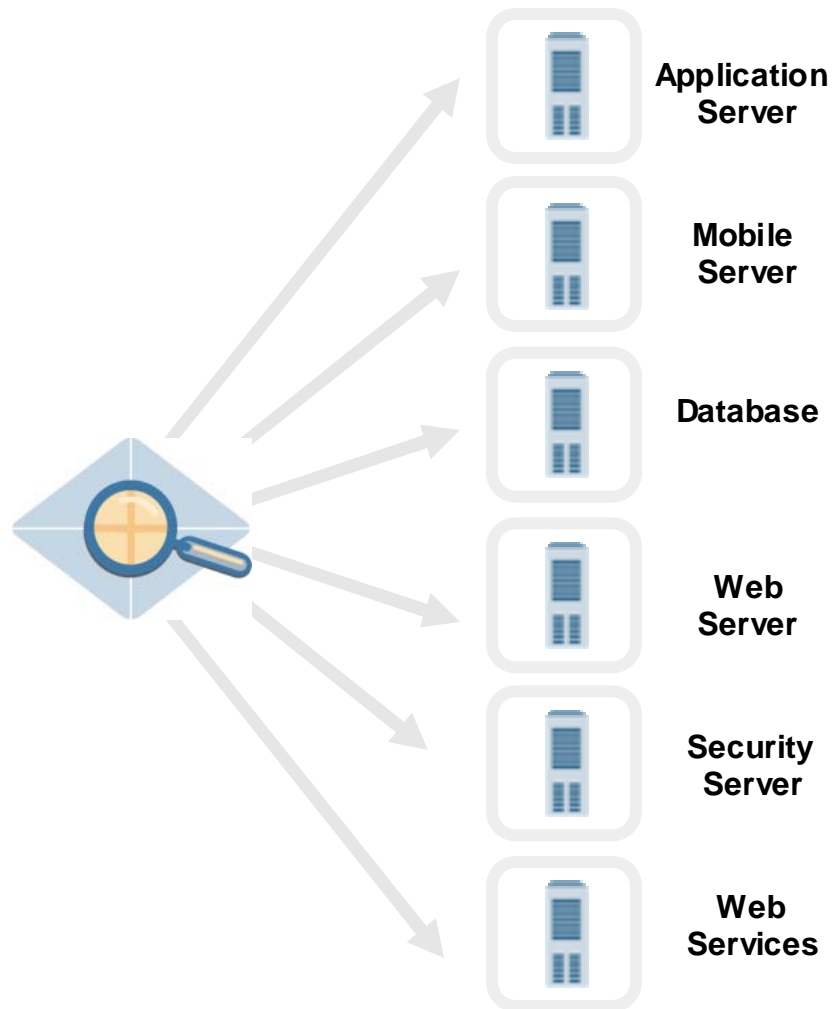
Or, Network Core?

- Internal/External attacks
- Application specific protection
- Transaction assurance
- Server and application load balancing
- URL and content transformation/masking
- Traffic optimization – SSL termination, compression

Application-specific security at the network core protects against internal/external attacks



Protocols

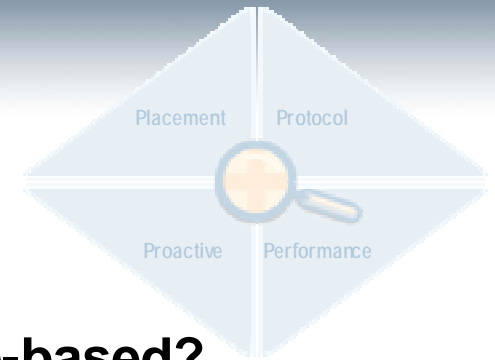


- **Web content...**
 - HTML
 - SOAP/XML
- **Plus, other applications...**
 - Database servers (SQL)
 - Mail servers (SMTP)
 - Terminal servers (RDP)
 - Mobile gateway (SIP, WAP)
- **Including, authentication methods**
 - Client certificates

Need Flexibility to support multiple protocols and authentication to ensure broad application security



Proactive



Application Profile	
Application Name	Online Banking We
Policy Name	Web Site Security
Cookie Policy	Strict Cookie Policy
Input Filter Policy	Form Field Check
Masking Policy	Web site mask
Authentication Policy	Online banking Auth
Authorization Policy	E-Banking Security Policy
<input type="button" value="Submit"/>	

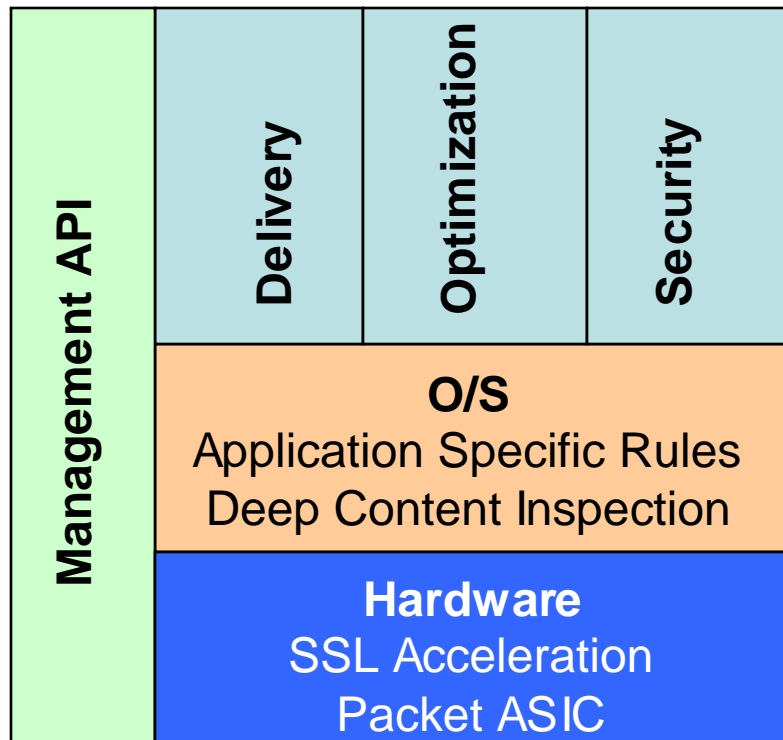
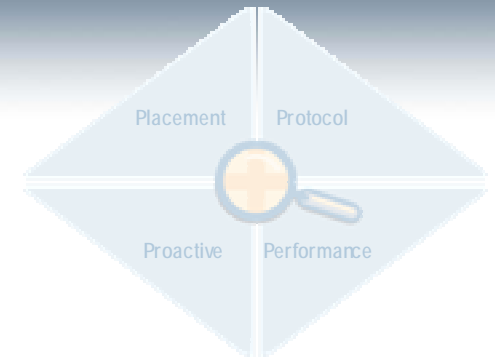


- **Signature-based?**
 - Attack database
 - Regular updates/patches
 - Negative, reactive model
- **Or, Application specific?**
 - Context aware of each application group
 - Validate data fields and other application specific content
 - Automatic learning (80-95%)
 - Full proxy architecture
 - Open API
 - Interface to applications
 - Proactive, positive model

Stopping Day Zero attacks requires a full proxy architecture & positive security model



Performance

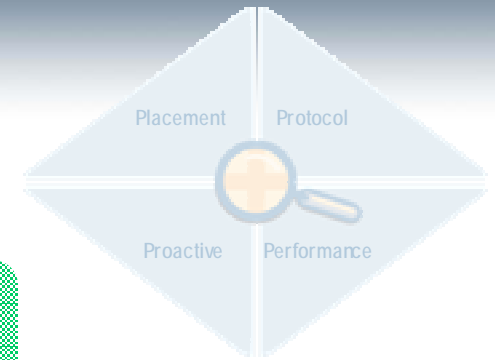


- **Hardware**
 - Powerful processing engine
 - SSL offload
 - Specialized ASIC
- **Operating system**
 - Optimized hardened kernel
 - Line-speed full proxy architecture
 - Low latency
- **Function**
 - Server/application traffic mgmt
 - Application optimization
 - Proactive application security

A specialized architecture is required for line-speed application security processing



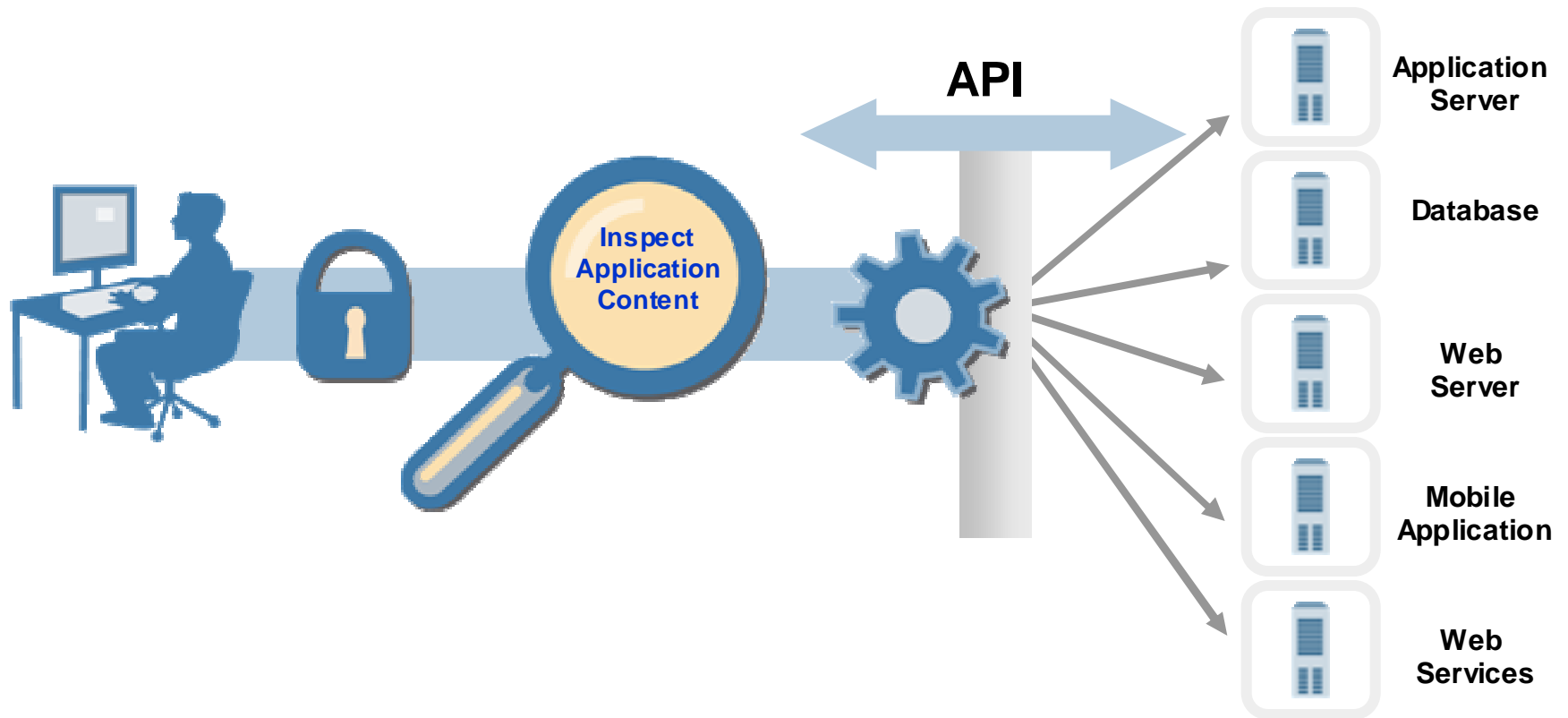
Local Traffic Manager



TRAFFIC
DECRYPTION

APPLICATION
SECURITY

DYNAMIC
RULES



Foundation for Application Security