Overview of F5 Networks

Fatih Bilger
Senior Systems Engineer, Prolink

fatih.bilger@prolink.com.tr
Company Snapshot

- Leading provider of Application Delivery Networking products that optimize the security, performance & availability of network applications, servers and storage systems
- Founded 1996 / Public 1999
- Approx. 2,130 employees
- FY09 Revenue: $653M
- FY10 Revenue: $882M
Who Is F5 Networks?

Value Innovation
- Unique TMOS architecture
- Industry’s only open iControl API & SDK
- Powerful iRules and DevCentral Community
- Numerous Industry Patents

Proven Results
- Over 16,000 Customers
- FY10 Revenue: $882 M
- #1 in Advanced Platform ADC Market – Gartner

Application Partnerships
- Unique F5 and application vendor integration
- Application partner tested and documented solutions
- F5 solutions in partner labs
- Cooperative Support Agreements

FORTUNE
List of 100 Fastest-Growing Companies 2010
Cyberattacks & web apps: motivation, methods and mitigation

Fatih Bilger
Senior Systems Engineer, Prolink

fatih.bilger@prolink.com.tr
The historic NeXT computer used by Tim Berners-Lee in 1990, on display in the Microcosm exhibition at CERN. It was the first web server, hypermedia browser and web editor.
The historic NeXT computer used by Tim Berners-Lee in 1990, on display in the Microcosm exhibition at CERN. It was the first web server, hypermedia browser and web editor.
The historic NeXT computer used by Tim Berners-Lee in 1990, on display in the Microcosm exhibition at CERN. It was the first web server, hypermedia browser and web editor.
The historic NeXT computer used by Tim Berners-Lee in 1990, on display in the Microcosm exhibition at CERN. It was the first web server, hypermedia browser and web editor.
Web Application Trends and Technologies

Web 1.0
- Audio & Video downloads
- File transfers

Web 2.0
- SOA
- SaaS
- AJAX
- Silverlight/Flex 3
- RIA
- Audio & Video streaming

Application Complexity
- Less
- More

Network Load
- High Traffic
- Low Traffic

Low Traffic
- Basic HTML
- Flat web pages

High Traffic
- facebook
- Google Maps
- myspace.com
- YouTube
Web Application Trends and Technologies

Web 2.0
- SOA
- SaaS
- AJAX
- Silverlight/Flex 3
- RIA
- Audio & Video streaming

Web 1.0
- Audio & Video downloads
- File transfers
- Basic HTML
- Flat web pages

Application Complexity
- Less
- More

Network Load
- High Traffic
- Low Traffic
Web Application Trends and Technologies

- Web 1.0
  - Audio & Video downloads
  - File transfers
  - Basic HTML
  - Flat web pages

- Web 2.0
  - SOA
  - SaaS
  - AJAX
  - Silverlight/Flex 3
  - RIA
  - Audio & Video streaming

Complexity is the Enemy of Good Security
Expanding Needs and Demands

- Globalization
- Flex Working
- Branch Expansion
- Mobility
- E-Commerce

- Green Datacenters
- Security/Compliance
- Business Continuity
- Web and Enterprise 2.0
- SaaS, XML, SOA
Where are the Weak Spots?

- Transport
- Browsers (Client Software)
- Error Codes and Server Responses
- Web Platform – IIS & Apache
- Application Servers
- Databases
- Web Application – Authentication, Authorization, Site Structure, Input Validation, App Logic & Management Interface
Almost every web application is vulnerable!

- “97% of websites at immediate risk of being hacked due to vulnerabilities! 69% of vulnerabilities are client side-attacks”
  - Web Application Security Consortium

- “8 out of 10 websites vulnerable to attack”
  - WhiteHat “security report ”

- “75 percent of hacks happen at the application”
  - Gartner “Security at the Application Level”

- “64 percent of developers are not confident in their ability to write secure applications.”
  - Microsoft Developer Research
Overall Top Vulnerability Classes
(Sorted by percentage likelihood)

Website Security Statistics Report from WhiteHat Security
Motives of Hackers

- Pursuit of fame or recognition
- Personal or Commercial Gain
- Malicious Intent – Causing severe damage to information & assets
- Terror – Cyber War
How long to resolve a vulnerability?

- Cross-Site Scripting: 58 days
- Information Leakage: 85 days
- Content Spoofing: 71 days
- Insufficient Authorization: 72 days
- SQL Injection: 38 days
- Predicable Resource Location: 79 days
- Session Fixation: 104 days
- Cross-Site Request Forgery: 56 days
- Insufficient Authentication: 125 days
- HTTP Response Splitting: 80 days

Average number of days for vulnerabilities to be resolved (sorted by class)
What does a vulnerability cost?

- The average custom business application has 150,000 to 250,000 lines of code
  -- Software Magazine

- Every 1000 lines of code averages 15 critical security defects
  -- U.S. Department of Defense

That means there are an average of 2,250 security defects in every business application!

- The average security defect takes 75 minutes to diagnose and 6 hours to fix
  -- 5-year Pentagon Study

That means 2,800 hours to diagnose the defects and 13,500 hours to fix them!

- Average worldwide cost of programmer = $40 per hour
  -- F5 Networks

- That’s a cost of $112k to diagnose the defects and $540k to fix the defects
Attacks are Moving “Up the Stack”

90% of security investment focused here

75% of attacks focused here

Source: Gartner
Network Firewalls vs. Application Firewalls

- **Network Firewalls**
  - Manage network traffic
  - Protection At Network Layer 3
  - Manage Access to Corporate LAN’s
  - Simple Forwarding Of Approved Packets

- **Application Firewalls**
  - Manage web traffic
  - Protection At Application Layer 7
  - Monitor HTTP/S & XML Protocols
  - Protect Application & Backend Data From Malicious Attack’s & Unauthorized Usage
  - Deep Packet Inspection Of All Traffic To And From The Web Servers

**Packet Inspection**

**Deep Stream Inspection**
Network Firewalls vs. Application Firewalls

Network Firewalls
- Manage network traffic
- Protection at Network Layer 3
- Manage access to Corporate LAN’s
- Simple forwarding of approved packets

Application Firewalls
- Manage web traffic
- Protection at Application Layer 7
- Monitor HTTP/S & XML protocols
- Protect application & backend data from malicious attacks & unauthorized usage
- Deep packet inspection of all traffic to and from the web servers

Packet Inspection

Deep Stream Inspection
Take a Proactive Strategy Based on Truths

### Myths
- Programmers Write Perfect Software
- Few and Simple Access Scenarios
- Data Theft Occurs at Network Level
- You Can Secure The Endpoint
- Users are Secure

### Facts
- Programmers Write Buggy Software
- Many and Varying Access Scenarios
- 75% of Data Theft is at the Application Level
- You Can Secure Access
- Users are Inherently Insecure
Application Firewall:
Deployment Architecture

Positive Security

Negative Security

What is Allowed

Applied Security

What is Denied
What is the value of web application Firewall?

- Reduce operation costs –
  - Ensure high application availability by stopping attacks
  - Reduce the expenses of meeting PCI security compliance requirements by showing clean scans
- Streamline application delivery
- Cut your infrastructure costs – consolidation
- Easy to deploy security policies
- Improve workforce efficiency
- Application visibility and reporting
- Handle changing threats with greater agility
Benefits

- **Developers** spend less time fixing security holes – freeing them up to spend more time building new business applications.

- **Security Professionals** can focus on solutions -- enforcing security policies and improving those policies. They spend less time fixing security holes.

- **Architects** can focus and improve the best practices for application availability, performance, and security.

- **Auditors** reduce the time required for security assessments and remediation.
Thank You !