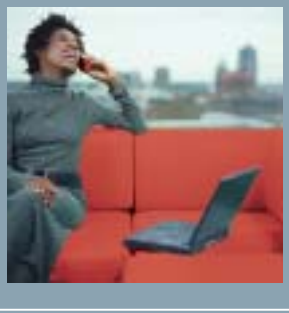
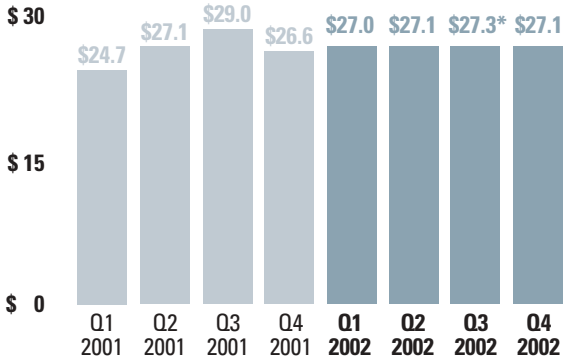


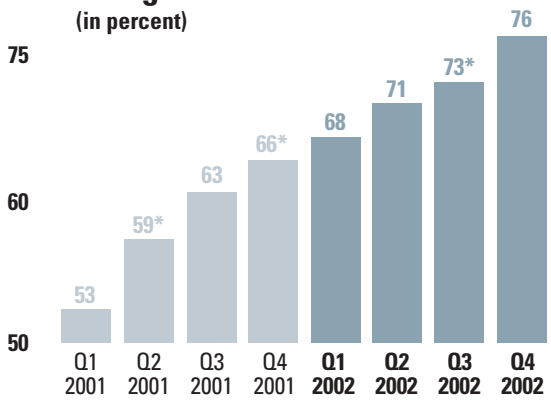
ANNUAL REPORT 2002

Selected Financial Data

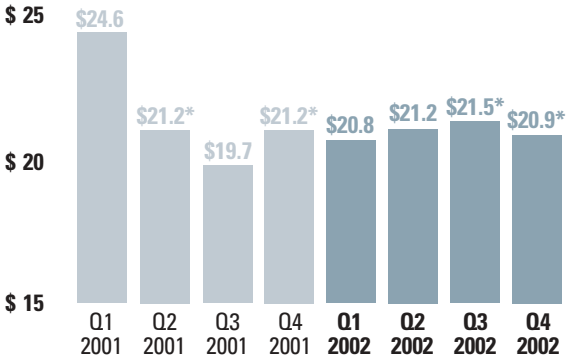
Net Revenue
(in millions)



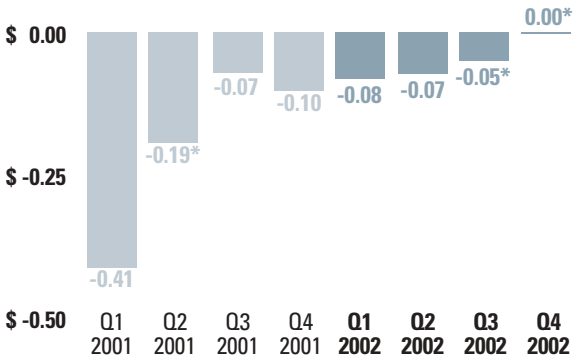
Gross Margin
(in percent)



Operating Expenses
(in millions)



Earnings Per Share (EPS)

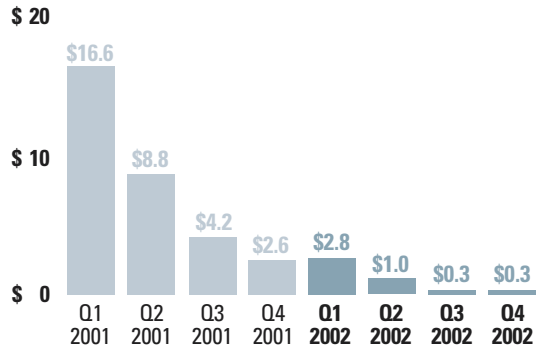


* Pro forma. A reconciliation of actual and pro forma results for each quarter is included in the company's quarterly income statements, available on our Web site at www.f5.com/f5/ir/reports/.

Selected Financial Data (in thousands)	2002 Actual	2002 Pro Forma	2001 Actual	2001 Pro Forma
Net Revenues	$ 108,266	$ 108,509	$ 107,367	$ 107,367
Gross Profit	$ 77,787	$ 78,368	$ 61,862	$ 65,057
Operating Expenses	$ 87,328	$ 84,391	$ 90,578	$ 85,801
Loss from Operations	$ (9,541)	$ (6,023)	$ (28,716)	$ (20,744)
Net Loss	$ (8,610)	$ (5,092)	$ (30,790)	$ (13,935)
Cash, Cash Equivalents & Investments	$ 80,333	$ 80,333	$ 69,783	$ 69,783
Long-Term Debt	$ 0	$ 0	$ 0	$ 0
Net loss as reported		$ (8,610)		$ (30,790)
Return reserve (contra product revenue)		243		
Write down of inventory (cost of net revenues)		338		3,195
Amortization of unearned compensation				1,300
Bad debt recovery (general and administrative)		(500)		
Bad debt (general and administrative)		163		2,000
Executive recruitment (general and administrative)				502
Restructuring charges		3,274		975
Income tax expense				8,683
Impairment of assets due to office relocation (other income, net)				200
Pro forma net income (loss)		$ (5,092)		$ (13,935)

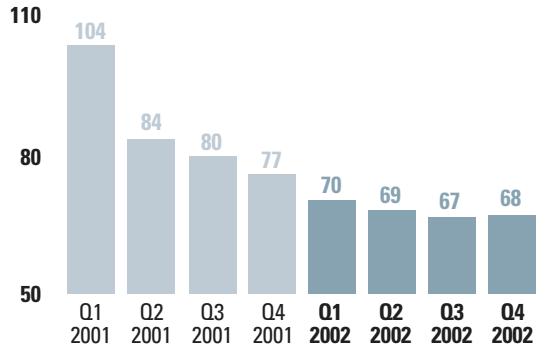
Inventories

(in millions)



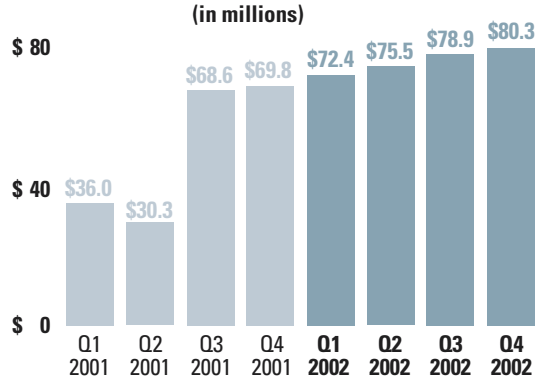
Days Sales Outstanding (DSO)

(in days)



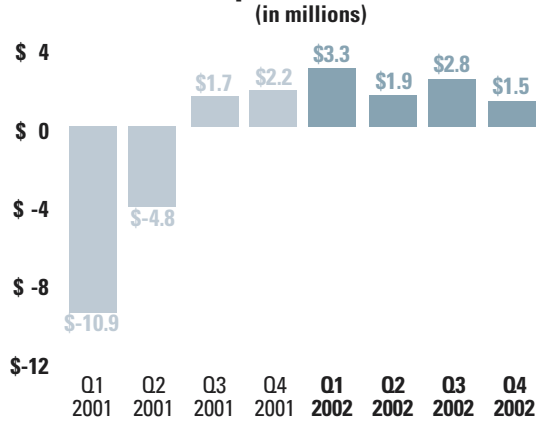
Cash and Investments

(in millions)



Cash Flow from Operations

(in millions)



F5 Networks is the leading provider of Application Traffic Management solutions for networks using the Internet Protocol. Built with a common software architecture (iControl™), our industry-leading products reduce the cost, improve the efficiency, increase the business security and boost the overall performance of IP-based enterprise networks, servers and the applications that run on them. Features of our BIG-IP® software enable our products to read the entire contents of IP packets, identify any value in those packets, and direct, filter or persist on the data according to customized rules generated by users and applications. BIG-IP software runs on a variety of Intel-based hardware platforms, including application switches and server appliances manufactured by F5 and our OEM partners and blade servers manufactured by a number of server vendors.

F5's products and services are sold to large enterprise customers worldwide through a variety of channels, including OEMs, Distributors, Value-Added Resellers (VARs) and System Integrators (SIs). In North America, we also sell to major accounts through our own field sales force. During fiscal 2002, we generated 76 percent of our revenue from product sales and 24 percent from maintenance and related services. Based on market data for the quarter ended September 30, 2002, F5 led the Layer 4/7 Fixed Switch and Appliance Market with 29 percent of total revenue.

F5 has approximately 475 employees in our Seattle, Washington, headquarters and offices throughout North America, Europe and Asia Pacific. Our address on the Web is www.f5.com.

This report should be read in conjunction with the company's Form 10-K for fiscal year 2002.

F5 Networks executive team. From left to right (*back)* Steve Goldman, Brett Helsel, Jeff Pancottine, Julian Eames, (*middle)* Steve Coburn, (*front)* Joann Reiter, John McAdam.

To Our Shareholders

Fiscal 2002 was a year of significant achievement for F5 Networks. The company successfully launched several new products and gained share in both the Layer 4/7 and SSL (Secure Socket Layer) markets. We expanded our base of enterprise customers and increased the volume of our business in major accounts. And we continued to fine-tune our operating model with resulting improvements in several key financial metrics.

Year over year, the company's revenue was up only slightly, from $107.4 million in fiscal 2001 to $108.3 million in fiscal 2002. During a period when many of our competitors reported declining revenues, however, I'm pleased that **we were able to sustain flat revenues across all four quarters.** Equally important, while we reported a net loss of $8.6 million ($0.34 share) for the year ($5.1 million or $0.20 per share pro forma), we pared our quarterly net loss to $423,000 ($0.02 per share) in the fourth quarter and **achieved breakeven results on a pro forma basis*.**

Just weeks before the beginning of fiscal 2002, we launched our first application switch product, BIG-IP® 5000, which was followed four months later by BIG-IP 2000. By the end of the second quarter, both products had come to represent nearly half of system sales. And by September 30, **our share of the Layer 4/7 fixed switch market had grown from zero a year earlier to 17 percent** (source: Dell'Oro). During the same period, combined sales of BIG-IP application switches and appliances increased **our share of the Layer 4/7 fixed switch and appliance market to 29 percent** (source: Dell'Oro/F5). Integrated SSL acceleration on both products also helped drive **our share of the market for Layer 4-7 Switch/Load Balancers with SSL to 79 percent** (source: Infonetics) for the first half of calendar 2002.

Weeks after the close of fiscal 2002, **we upgraded and expanded our application switch family with the introduction of three new products:** BIG-IP 5100 combines industry-leading Layer

* Pro forma net income for the fourth quarter of fiscal 2002 excluded a one-time restructuring charge of $503 thousand related to F5's exit from the cache business, announced on July 8, 2002. A reconciliation of annual pro forma items to actual results is provided on page 1 of this report.

7 performance and Layer 4 traffic management with 24-port Layer 2/3 switching and integrated SSL; BIG-IP 2400 combines Layer 7 traffic management, 16-port Layer 2/3 switching and integrated SSL with a new custom-designed ASIC (application specific integrated circuit) that delivers the industry's fastest Layer 4 performance; and BIG-IP 1000 combines Layer 4/7 traffic management with 8-port Layer 2/3 switching to deliver the most cost-effective application traffic management solution on the market. These products significantly enhance our ability to meet the various needs of our enterprise customers and have received favorable reviews in the trade press and from industry analysts. In its December 2, 2002 issue, for example, **InfoWorld called the new products "a real plus for companies that need to optimize their network efficiency."**

A common feature of all three products is version 4.5 of BIG-IP's Layer 7 application traffic management software. Key components of the new software are the Universal Inspection Engine (UIE), which enables BIG-IP to identify any value of an IP packet, and iRules, which allow users to easily write custom business rules that use those values to direct, filter or persist traffic to and from servers and applications. In combination, **UIE and iRules give customers unprecedented power and flexibility to manage virtually any type of IP-based application traffic,** from instant messaging and voice-over-IP to database requests and XML tags used in Web services.

In addition to UIE and iRules, version 4.5 incorporates **a new feature called Dynamic Security Control Architecture (DSCA)** that enhances the security capabilities of our products. Integrating SSL acceleration with Layer 7 traffic management has been a key driver of BIG-IP application switch sales. Encrypting and de-encrypting data on BIG-IP is faster and less costly than doing it on a server. And it allows UIE to examine the data and apply iRules before sending it on. With DSCA, BIG-IP has the capability to interface directly with intrusion detection systems and other network security devices, enabling them to block security threats quickly and eliminating the need for manual intervention. **This has significantly expanded our addressable market.**

Within the market for Layer 7 traffic management, we believe our **software-based technology offers customers a superior alternative to competing hardware-based products.** Frequent updates, which aren't feasible in hardware-based solutions, allow us to keep pace with the adoption of new protocols and emerging trends such as Web services. As exemplified in UIE and iRules, our software also allows customers to adapt our traffic management solutions to their specific business needs. And through iControl™, our SOAP/XML interface, IP-based applications themselves can communicate directly with our products to control the network and optimize their performance.

Throughout fiscal 2002, **we continued to forge and strengthen partnerships with major software vendors such as Microsoft, Oracle, BEA, Hewlett Packard and Web Methods,** who have enabled their applications to interface with iControl. During the fourth quarter, we estimate that approximately 15 percent of our system sales involved at least one iControl partner.

In terms of market opportunity, **the portability of our software-based solutions gives F5 an important edge over our competitors.** Although 93 percent of our product revenue in fiscal 2002 was derived from system sales, 7 percent came from licensing our software to original equipment manufacturers (OEMs) and end users. The majority of licensing revenue during the year was from Dell, which resells our software on its own line of server appliances. During the second fiscal quarter, Nokia also began contributing OEM revenue, which grew modestly over the next two quarters. Going forward, we anticipate that the percentage of software sales in our revenue mix will increase as OEM revenue is augmented by software licensing revenue from sales of BIG-IP Blade Controller.

Introduced in May 2002, Blade Controller is a version of the **BIG-IP software modified to run on new blade server platforms from Dell, Fujitsu-Siemens, Hewlett Packard, IBM and RLX Technologies.** During the second half of fiscal 2002, we sold a modest number of Blade Controller licenses into the nascent blade server market. With the first products from Dell and IBM just beginning to enter the

market, **we anticipate that we will see our first significant sales of Blade Controller in the first half of calendar 2003.** In the meantime, we are continuing to work closely with each vendor to develop individualized marketing programs to target their customer base.

In addition to broadening and enhancing our product offerings in fiscal 2002, **we continued to widen our base of enterprise customers and grow our business in major accounts.** In the second half, we also began to see an increase in sales to providers of wireless communications. During the year, revenue from major accounts grew significantly, with sales to our nine largest accounts approaching $13 million for the year, up from less than $3 million for those same accounts in fiscal 2001. Geographically, North America was our strongest market, with Europe up and Japan down slightly year over year.

Our success in selling to enterprise customers highlights the strength of our technology in addressing their business needs. To a lesser degree, it also reflects **significant improvements in the company's operating model and balance sheet** that have reinforced our strong market position.

Driven largely by the consolidation of our system platforms and improved manufacturing efficiencies, pro forma* **gross margin increased from 60.6% in fiscal 2001 to 72.2%** in fiscal 2002 while pro forma **operating expenses declined from $85.8 million to $84.4 million** during the same period. Part of the improvement in these metrics resulted from our decision to exit the cache business and scale back our workforce in July.

In terms of asset utilization, the quality of our enterprise accounts was a key factor in reducing **days sales outstanding (DSOs) from 77 days a year ago to 68 days** at year end. As a result of this and other factors, including aggressive inventory management, **we generated nearly $10 million in cash flow from operations** during the year, increasing our cash and investments from $69.8 at the end of fiscal 2001 to **$80.3 million at the end of fiscal 2002.**

As a result of these improvements and our increasing market share, we believe F5 is well positioned

* A reconciliation of annual pro forma items to actual results is provided on page 1 of this report.

to weather a continuation of the current business cycle and to benefit from any upturn in corporate spending. With or without any improvement in the economy, however, **our primary goal during fiscal 2003 is to drive the company's revenue growth by focusing on those market opportunities for which our technology is best suited.** In addition to our unique position in the blade server market, those opportunities include the continued rollout of IP-enabled enterprise applications, the ongoing development of wireless Internet infrastructure, the growing need for improvements in network security, and the accelerating development of Web services.

On behalf of the entire company, **thanks for your support** of our efforts to make F5 Networks the undisputed market leader in Application Traffic Management for the enterprise.

John McAdam

President and

Chief Executive Officer

November 30, 2002


POWER
STATUS
ACTIVITY
ALARM

Application Traffic Management

F5 Networks pioneered the category of load balancing with the introduction of BIG-IP® in 1997. At that time, the issue of managing traffic associated with the rapid deployment of Web servers was a major challenge and BIG-IP was the answer. Through subsequent enhancements to BIG-IP, F5 helped transform the industry by adding network intelligence and the ability to manage Web-enabled applications. Today, BIG-IP can manage traffic for any type of application over any network that uses the Internet Protocol (IP). We call this capability Application Traffic Management and it is already changing the way people and applications view the network.

BIG-IP products perform basic switching and routing functions, monitor the health of networks, enhance network security, ensure high availability of applications and servers, simplify the deployment of new applications and reduce the cost and complexity of network administration. As a result, F5 is strategically aligned with several emerging trends—such as Web-enabled enterprise applications, mobile Internet applications, and Web services—that industry analysts expect to drive the growth of Internet-related technology for the next three to five years.

In terms of the Open Systems Interconnect (OSI) Reference Model, the framework that describes and defines how networked systems communicate with one another, the core of BIG-IP is sophisticated software that manages IP traffic at Layer 7, also known as the application layer. The F5 BIG-IP application switches also perform Layer 2/3 switching and industry-leading Layer 4 switching. But it is the superior performance and functionality of the BIG-IP Layer 7 traffic management software that has distinguished them from competing products sold by Cisco Systems, Nortel Networks, and others.

In contrast to the tasks associated with Layers 2 - 4, Layer 7 functionality is complex and variable. Switching devices for Layers 2 - 4 merely ensure that packets of information sent over the Internet arrive at the destination to which they are addressed, and that they are reassembled in the correct sequence. In many ways, the kinds of functions carried out at Layers 2 - 4 are analogous to those carried out by the postal service in picking up and delivering mail. Layer 7 corresponds to preparing and reading the contents of the mail and to the interaction between the sender and receiver.

When mail is sent through the postal system, different kinds of documents and packages from various sources can be designated for delivery to a single individual at a specific address; for example,

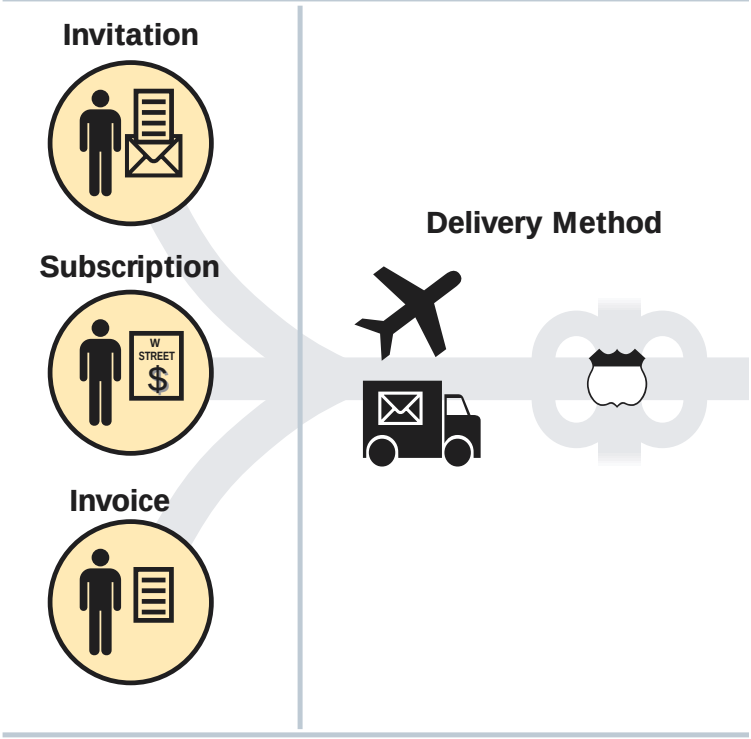
Abigail Baker
Chief Financial Officer
Charlie Company
123 D Street
Emerald City, Kansas 64321

On a typical day, a number of individuals and organizations—including those within Charlie Company—might send Ms. Baker many different types of mail:

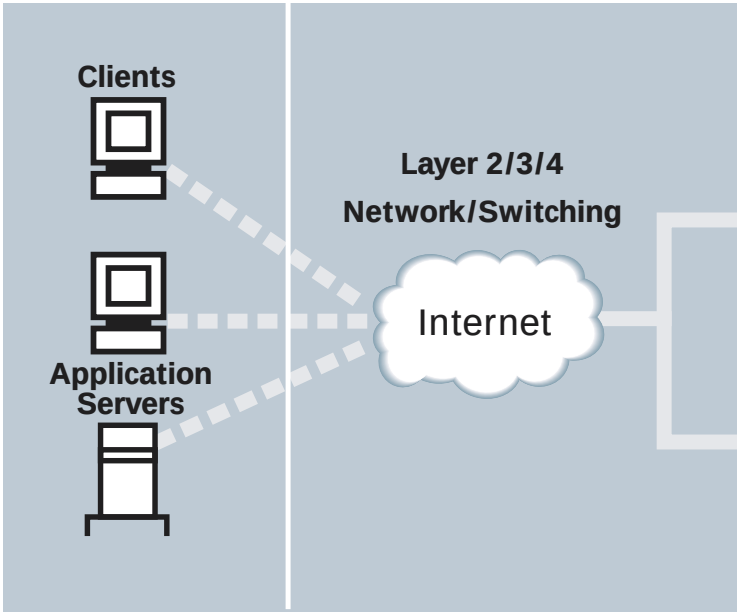
- An invitation to a partner's product launch
- A subscription renewal notice from the *Wall Street Journal*
- An invitation to attend an investment seminar
- The monthly statement for her corporate credit card
- This week's copy of the *Economist* magazine
- A copy of a new report on the company by a brokerage firm analyst
- The final draft of a job offer to a new Controller that requires her review and signature (sent from HR via inter-office mail)
- The first draft of a letter of intent for a joint venture, sent by the prospective partner's attorneys via overnight courier

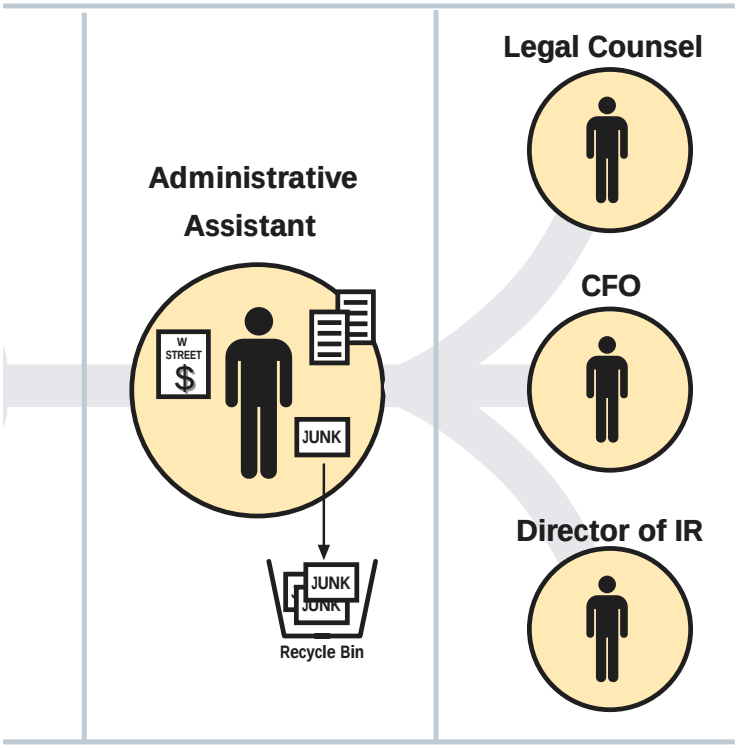
Although each item is prepared in a specific way for a specific purpose, they all go through a similar process to get to Ms. Baker. Each is packaged and addressed using a standard format. Postage or a delivery fee is determined and paid. Then, each packaged and addressed

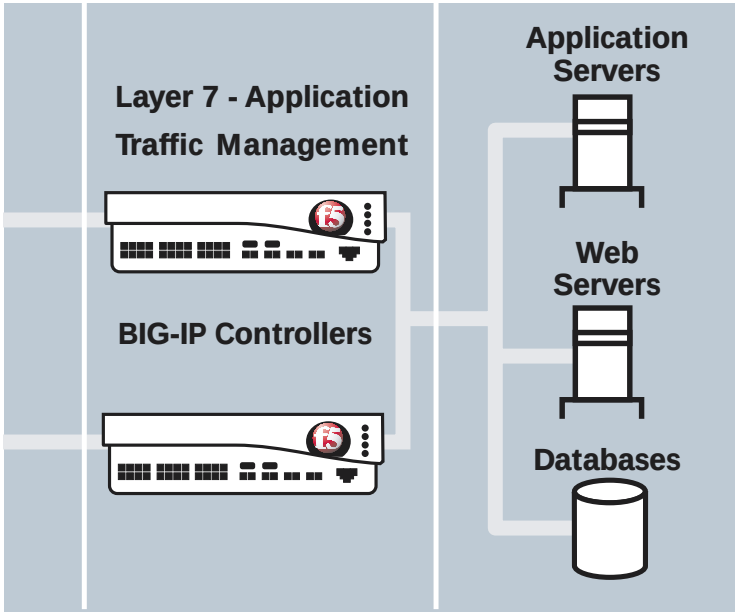
Intelligent Delivery of Mail



Intelligent Delivery of IP Packets







item is handed off directly, or indirectly, to a postal or delivery service employee.

Once in the postal or delivery service system, each piece is physically transported over various distances, working its way through a series of processes that aggregate thousands of pieces addressed to employees of Charlie Company before delivering them to the company's mail room. Finally, mail that has been sorted by department or mail stop and combined with special deliveries and interdepartmental mail is delivered to employees who place it in individual mailboxes.

Ms. Baker doesn't open or respond directly to all the mail sent to her. Her administrative assistant opens most of it and handles each piece according to a set of variable rules that reflect his knowledge of Ms. Baker and her preferences, specific instructions she has given him, and any special circumstances that arise.

As he sorts through the mail, Ms. Baker's assistant turns his attention first to the final draft of the job offer and the letter of intent. He knows Ms. Baker is expecting both of these documents, but this morning she told him she wanted George Fox, the company's in-house counsel, to review the job offer one more time before she signs it. Accordingly, he carries it over to Mr. Fox and hands it to him. Ms. Baker is away from her desk, so he places the letter of intent face down on her chair.

Next, he checks Ms. Baker's calendar to see if she is free to attend the partner launch. Since

she is, he blocks out the date and time on her calendar, attaches a note to the invitation asking if she wants to attend, and puts the invitation in her inbox. Since he already knows she wants to continue her subscription to the Wall Street Journal, he signs her up for a one-year renewal, billing it to her corporate credit card and making a note to add it to this week's expense report that he will prepare for her. Ordinarily, Ms. Baker's assistant would put this week's Economist on her credenza, along with other recent magazines. But since one of the stories in this week's issue is about one of Charlie Company's largest customers, he marks the page with a sticky note and puts it in her inbox.

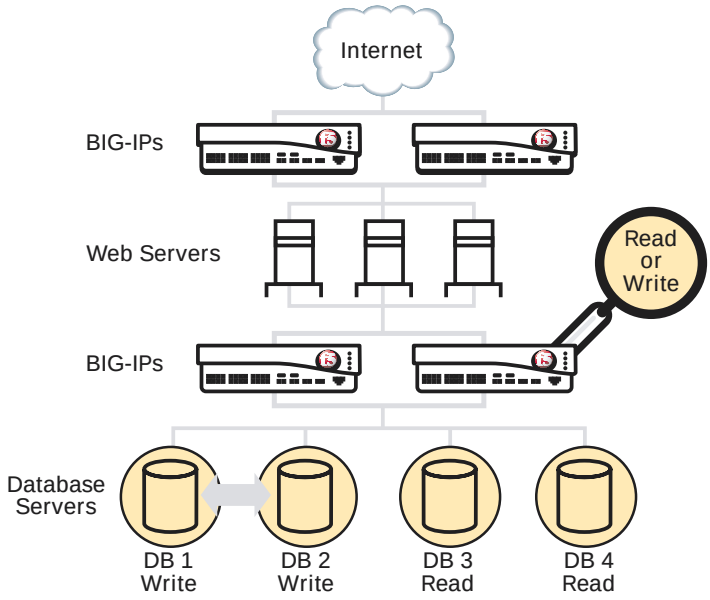
Even though the analyst report is addressed to Ms. Baker, she has instructed her assistant to route all investor relations materials directly to the Director of IR. Accordingly, he puts the report in the Director's mailbox.

Under Ms. Baker's working definition of "junk mail", the invitation to the investment seminar qualifies and is consigned to the recycling bin.

Although the correspondence is far from exact, there are a number of parallels that can be drawn between this example and application traffic management. The senders of all the pieces intended for Ms. Baker correspond to various client systems connected to the Internet or to Charlie Company's Intranet. Ms. Baker herself corresponds to several different applications running on a group of servers. The preparation of each piece by the sender and the response it generates in Ms. Baker's office are analogous to what goes on at the application layer (Layer 7) when data is exchanged between clients and applications over IP-based networks. The functions performed by Ms. Baker's assistant correspond to the application traffic management functions of BIG-IP. Ms. Baker could perform

Enterprise Application: Database Scaling

A large transportation/logistics company in the US needs a cost-effective way to scale and provide high availability for its customer record databases. Since 90 percent of the traffic represents read-only requests, adding more large servers with the kind of sophisticated replication software needed for write transactions is an expensive option. Instead, they could install BIG-IP application switches in front of the database servers and scale their read-only databases with less expensive servers and replication software. Because UIE can recognize and distinguish between read and write commands, an iRule could be written to direct each to the appropriate group of servers.



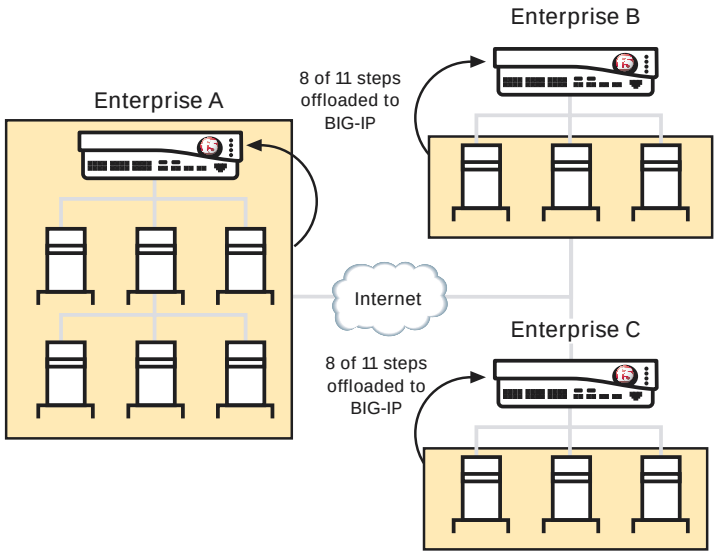
those functions herself. But it's a much more efficient use of her time to have her assistant do them for her. In the same way, many Layer 7 functions can be performed on a server or written into an application, but it's much more cost-effective to deploy BIG-IP. In addition, BIG-IP performs many functions that would be impractical to host on a server or build into an application.

As IP packets from various sources arrive at their destination and are reassembled, BIG-IP's Universal Inspection Engine (UIE), enables it to read the contents of the packets and make intelligent decisions about where and how to send each transmission to optimize the performance of the network, network servers and the applications running on them. Integrated SSL (secure socket layer) acceleration enables BIG-IP to decrypt secure transmissions before deciding where and how to send them on, and BIG-IP can also insert other data into packets to ensure that transmissions are sent to the most appropriate resource. In addition, BIG-IP's iControl architecture enables it to communicate directly with applications through a SOAP/XML interface that lets the applications control the network dynamically, saving time, money and resources.

The decisions made by BIG-IP are based on a new feature of the software called iRules, which includes a set of standard rules for routing traffic and allowing customers to add their own business rules. Standard rules include checking the target server and application to make sure that both are available and operating correctly before sending traffic to them. Custom rules can govern how traffic is to be managed with reference to virtually any element or group of elements within a transmission. At one US airline, for example, BIG-IP is used to manage the flow of traffic to and from servers that

Web Services Application: Security

A US manufacturer with approximately 50 suppliers worldwide wants to develop a secure Web service to replace the current process of communicating with them via paper, fax, phone and email. A major stumbling block is that secure Web services transactions require 11 separate steps (generate the request; insert a digital signature; insert a client certificate; encrypt the traffic; decrypt the traffic; validate the client certificate; validate the digital signature; authorize the transaction; log the event; direct traffic to the appropriate resource; respond to the request) that would have to be built into the application at the customer site and at each supplier site. The cost and difficulty of doing this and maintaining the degree of consistency and reliability necessary to make the application work is prohibitive. However, the manufacturer could remove this obstacle by using BIG-IP application switches to manage the flow of traffic between them and their suppliers and offloading 8 of the 11 steps to BIG-IP. This would make deployment and maintenance of the Web service feasible and concentrate security in a centralized resource.

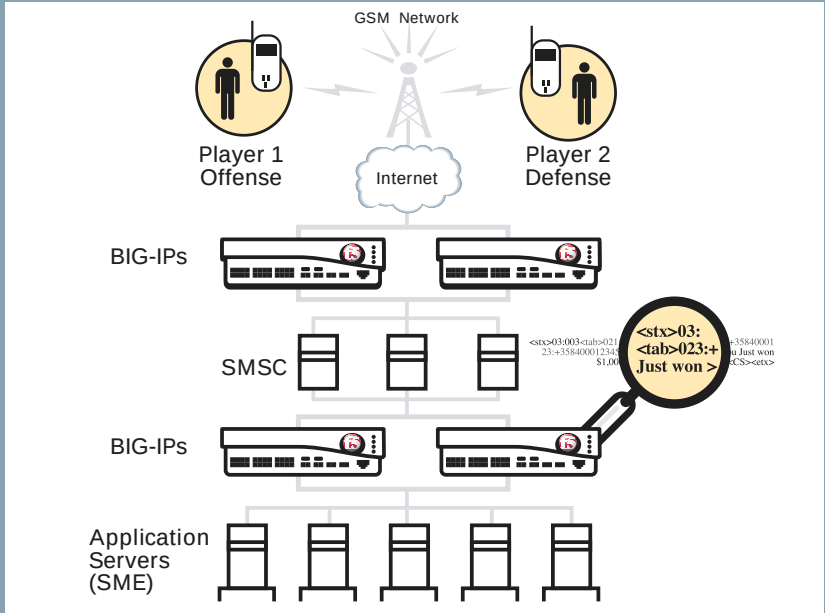


provide online services for frequent fliers. As transmissions come in, BIG-IP can identify the status of users from their member ID and send traffic from premier members to a special server where they receive priority service. At a major Japanese provider of wireless Internet communications, all traffic between the network and its 30 million users passes through BIG-IP devices that can identify the cell phone number of the caller. iRules uses this information and a feature called "persistence" to ensure that once a user begins a transaction on a particular server, he will stay connected to that server until the transaction is complete. If he should become disconnected before he is finished, BIG-IP allows him to reconnect to the same server and resume the transaction where he left off.

Because UIE can recognize any element of a packet, BIG-IP can be used to manage traffic for any type of IP-based application, including enterprise applications such as CRM (customer relationship management), database applications, mobile and wireless applications and Web services. At a large transportation company in the US, for example, BIG-IP might be used to distinguish between read and write traffic to its database servers, enabling the company to save money by purchasing less expensive servers to handle the read traffic. For a US semiconductor manufacturer, BIG-IP's ability to read XML data could enable it to implement a secure, centrally-managed Web service to communicate with approximately 50 suppliers world wide. In Northern Europe, BIG-IP's ability to manage wireless traffic could permit a government agency to expand a popular lottery game by ensuring that two players will remain connected to the same server for the duration of the game. As a result, the agency could accommodate more players

Mobile Application: Reliability and Scale

A popular European lottery game allows two individuals to compete for a lottery ticket by playing a game of football (soccer) over their cell phones. In order for the game to work, the two players must connect and persist (stay connected) to the same server. With a limited number of players, this did not present a problem, but as the number of players has increased the agency and its mobile operator need to figure out a cost effective way to scale the application and still ensure that every pair of players remains on the same server until the conclusion of their game. One option is to buy a much larger and more expensive server. A more cost-effective option that would allow far greater scalability is to install an array of inexpensive servers with the same application running on each, and a BIG-IP application switch to manage traffic in front of the servers. Because UIE can recognize any value in a transmission, network administrators could write an iRule forcing transmissions from any two players to persist to the same server. In addition, BIG-IP could balance the load of incoming calls and ensure high-availability by constantly monitoring the health of servers and applications.



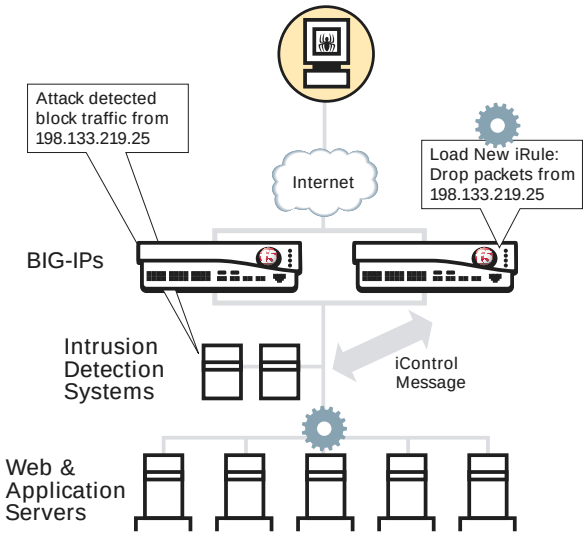
by replicating the game on many small servers, rather than hosting it on a single, large server with limited capacity. In the area of security enforcement, iControl™ and a feature of BIG-IP called Dynamic Security Control Architecture (DSCA) allow BIG-IP to work in conjunction with intrusion detection systems (IDS) that monitor the network for security threats. Rather than notify network managers when a security threat is detected, the IDS can communicate directly with BIG-IP which instantly generates a dynamic iRule to block or divert all traffic from the source of the detected threat.

BIG-IP's superior ability to manage the complex decision-making required at Layer 7 distinguishes it from other traffic management products. Because the majority of competing products are based on proprietary hardware and do not have the flexible software features of BIG-IP, their traffic management functionality is limited, preventing them from interacting dynamically with network applications.

BIG-IP application switches use commodity components for Layer 2/3 switching and a custom ASIC (application specific integrated circuit) we developed ourselves for Layer 4 switching. Since the company was founded, however, we have been committed to the development of a software solution as the only way to address the dynamic and increasingly complex requirements of application traffic management for Layer 7. With the recent introduction of BIG-IP version 4.5, we have continued to widen the gap between F5 and competing vendors of traffic management solutions.

Enterprise Application: Security Enforcement

Intrusion Detection Systems (IDS) are deployed in enterprise networks to monitor traffic and detect security threats such as denial-of-service attacks. In most implementations, the IDS responds to a perceived threat by identifying the source and sending an alert to a network administrator who must then issue a command shutting off traffic from that source. In the case of a real attack, this process can take several minutes under the best circumstances. In addition, the IDS frequently mistakes malformed packets for malicious transmissions, resulting in a number of false alerts. By deploying BIG-IP in conjunction with the IDS, false alerts could be eliminated and the process of shutting down an attack could be sped up significantly. BIG-IP screens all incoming traffic and could identify and drop all malformed packets before they reached the IDS. If an actual threat were detected, the IDS could alert BIG-IP directly through the iControl interface, and BIG-IP could instantly generate an iRule to drop all traffic coming from the source of the attack.



Shareholders' Information

Corporate Officers

John McAdam
President and Chief Executive Officer

Steve Coburn
Senior Vice President of Finance and Chief Financial Officer

Steve Goldman
Senior Vice President of Sales and Services

Brett Helsel
Senior Vice President of Product Development and Chief Technology Officer

Jeff Pancottine
Senior Vice President of Marketing and Business Development

Julian Eames
Senior Vice President of Business Operations and Vice President of Global Services

Joann Reiter
Vice President and General Counsel

Notice of Annual Meeting

Our annual shareholders meeting will be held:
F5 Networks Corporate Headquarters
February 13, 2003
10:00 AM

Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
206.272.5555
www.f5.com

Board of Directors

Jeffrey Hussey
Founder

John McAdam
President and Chief Executive Officer

Alan Higginson
President and CEO, Hubspan, Inc.

Karl Guelich
Certified Public Accountant

Keith Grinstein
Partner, Second Avenue Partners

Kenny Frerichs
Vice President, Business Development, Nokia Internet Communications

NASDAQ Listing

NASDAQ Symbol – FFIV

Investor Relations

206.272.6677
info@f5.com

Independent Accountants

PricewaterhouseCoopers LLP
Seattle, WA

Transfer Agent

American Stock Transfer
212.936.5100

The statements contained in this report that are not purely historical are forward-looking statements. These statements include, but are not limited to, statements about our plans, objectives, expectations, strategies and intentions and are generally identified by the words “expects,” “anticipates,” “intends,” “plans,” “believes,” “seeks,” “estimates,” and similar expressions. Because these forward-looking statements are subject to a number of risks and uncertainties, our actual results could differ materially from those expressed or implied by these forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, those discussed under the heading “Risk Factors” in the company’s Form 10-K for fiscal 2002 and in other documents we file from time to time with the Securities and Exchange Commission. All forward looking statements included in this report are based on information available to us on the date hereof. We assume no obligation to update any such forward-looking statements.

F5 Networks, Inc. • 401 Elliott Avenue West • Seattle, WA 98119 • 206.272.5555 • www.f5.com