F5 NETWORKS IT DEPARTMENT

"BIG-IP ASM enables us to see the IP addresses of all devices, so we can detect security threats, whether they're coming from IPv4 or IPv6 devices."

Casey Scott, Network Engineer at F5 Networks

F5 Supports IPv6 on Core Network; Maintains Security, Access Control while Cutting Costs

Since 2007, the **F5** IT team has worked to provide full support for IPv6 on the company's corporate infrastructure. In 2011, the team successfully established F5's public-facing web properties on the IPv6 Internet; in 2012, it focused on enabling IPv6 throughout the core network.

By deploying the latest F5® BIG-IP® products, the IT team provides remote users with secure access to IPv6-based corporate resources, protects the company's IPv4 and IPv6 production networks with advanced firewall capabilities, and enables remote teams to collaborate directly via IPv6. At the same time, the IT team was able to eliminate unnecessary hardware devices, simplify the infrastructure, and reduce capital and operational costs.

Business Challenges

In 1981, no one predicted that the demand for Internet Protocol version 4 (IPv4) addresses—required to identify all computers and devices connecting to the Internet—would far outpace supply just over a decade later. Internet Protocol version 6 (IPv6), supporting more than 340 trillion addresses, meets the ever-growing demand for IP addresses. However, because the two protocols are entirely incompatible, organizations worldwide must begin supporting IPv6 or risk eventually being

cut off from the "new world"—the IPv6 Internet and users of IPv6 mobile devices.

Since 2004 when F5's core technology, the BIG-IP product family, began natively supporting IPv6, F5's IT team has steadily worked to incorporate IPv6 support in the company's core network and IT infrastructure. The team obtained IPv6 addresses for F5 web properties in 2007, IPv6 circuits in 2008, and it has conducted three proof-of-concept projects since 2008. In June 2011, the team successfully

Overview

Industry
Technology

Challenges
· Provide secure, reliable SSL VPN service to IPv6
· Protect corporate resources on IPv6
· Enable collaboration among remote teams on IPv6
· Implement IPv6 without increasing infrastructure costs

Solution
· BIG-IP® Edge Gateway™
· BIG-IP® Access Policy Manager®
· BIG-IP® Application Security Manager™

Benefits
· Gives employees ubiquitous access to IPv6 corporate resources
· Protects corporate IPv6 resources from security threats
· Enables remote development teams to collaborate via IPv6
· Requires no additional infrastructure costs

demonstrated F5's "IPv6-readiness" by making f5.com web properties available on the IPv6 Internet for the first World IPv6 Day. While some vendor participants' sites scarcely remained live throughout the day, F5 web properties have remained continuously available on the IPv6 Internet for more than a year. "We never intended to turn off our IPv6-based web domains," says Casey Scott, Network Engineer at F5 Networks. "Our goal is to continually improve and expand our support for IPv6, both internally and externally."

The team's progress, which was captured in a **2011 F5 case study**, demonstrated that supporting IPv6 is not difficult for IT organizations and, in fact, can be implemented gradually using F5 solutions. "F5 customers can configure their BIG-IP devices for IPv6 without disrupting day-to-day operations, changing their security posture, or modifying their critical line-of-business applications, many of which do not yet support IPv6 natively," says Scott.

"This year, we've focused on providing a higher level of IPv6 service that benefits employees, internal organizations, and the company as a whole," Scott says. "We're making sure the company runs to the best of its ability on the IPv6 network—that's the next challenge our customers will be facing, too." For its fourth IPv6 proof of concept, the IT team addressed three specific needs:

- **Provide secure, reliable SSL VPN service to IPv6.** F5's large mobile workforce has secure remote access to resources on the company's core IPv4 network; the IT team wanted to provide secure access to its IPv6 network and resources as well. This requirement became particularly important in 2011 when F5 began offering IPv6 Solution Services to help customers implement IPv6 in their own IT environments. "We didn't want an F5 engineer to be stuck in a hotel room somewhere in Chicago or Tokyo without access to the IPv6 world," says Scott. "Our engineers must have reliable access to whatever resources they need so they can provide the best possible service to

"…we're able to deliver a business solution that gives employees…SSL VPN access to both the IPv4 and IPv6 worlds…"

our customers, no matter where they are in the world or what kind of network service is available locally."

- **Protect corporate resources.** F5's IT team wanted to provide the same level of security for its IPv6 environment that it provides for its core (IPv4) network. For its proof of concept in 2011, the team used a BIG-IP device as a gateway to proxy IPv6 traffic to IPv4, proving that IPv6 clients could reach the IPv4 Internet and IPv4-based applications. But whenever traffic goes through a gateway, the ability to see the source IP addresses is lost; instead, only the virtual IP address of the gateway device itself can be seen.

"That meant we couldn't detect attacks by IPv6 client devices—or even identify legitimate traffic that only appeared to be a security threat," said Scott. "Because of the security vulnerabilities introduced by proxying IPv6 traffic to IPv4, we never considered it a permanent solution. Before we could support IPv6 on our core network, we needed a way to see those the IP addresses of every client device."

- **Provide secure collaboration among remote teams.** Many remote development and engineering teams at F5 operate on IPv6 and want to have secure direct access to one another via the IPv6 networks, and to the IPv6 global Internet. "We wanted to eliminate 'islands of service' so our remote teams could share information easily and securely across IPv6 networks," says Scott. "We had evaluated third-party

firewall devices at the edge of our networks to establish IPsec tunnels for that traffic, but we wanted to provide IPsec connectivity and WAN optimization for IPv6."

Finally, the F5 IT team wanted to transition from its proof-of-concept implementation so it could load balance IPv6 traffic between application servers in its Seattle and Spokane data centers. To do that, however, the Seattle location had to be able to deliver the performance necessary to support F5's internal organizations as well as its public-facing sites. At 1.5 megabits per second, the existing T1 IPv6 circuits in Seattle were too slow to use in a production environment, but at the time, T1 was all that was available from the local internet service provider (ISP). The IT team needed more bandwidth to handle IPv6 traffic, which already accounted for about 10 percent of overall traffic and was expected to steadily increase over the next few years.

Solution

To meet these requirements, the IT team continued on its path of deploying the latest versions of F5 products. With the release of BIG-IP version 11.1 in late 2011, all major BIG-IP product modules are now IPv6-compliant. For policy-based access control both inside and outside of the corporate perimeter, the IT team deployed BIG-IP Access Policy Manager (APM). The team also deployed the latest version of BIG-IP Application Security Manager (ASM) to provide comprehensive web application firewall capabilities. Finally, it used BIG-IP Edge Gateway to facilitate IPv6 communication between remote development and engineering teams.

In addition, the IT team obtained a faster IPv6 circuit from F5's Seattle-area ISP, which was critical to its ability to support IPv6 in the company's core network. "IPv6 circuits are more readily available today from a broader range of ISPs, and they're more affordable," says Scott. "That was a hurdle for us before, but the offerings from ISPs have changed dramatically in just one year."

Benefits

As a result of these deployments, F5's IT team met the objectives of the proof of concept, reduced its IT infrastructure costs by eliminating unnecessary network devices, and once again demonstrated solutions that address real-world challenges that F5's customers face.

Provides secure, reliable access to IPv6 corporate resources

Accustomed to having secure remote access to corporate resources on IPv4, F5's mobile workforce now has secure access to IPv6-based corporate resources as well, thanks to BIG-IP APM version 11.1. A high-performance access and security solution, BIG-IP APM brings remote, LAN, and wireless connections together under a single management interface and enables granular, context-aware policy control.

"Because BIG-IP APM fully supports IPv6 now, we are able to deliver a business solution that gives employees—F5 engineers in particular—SSL VPN access to both the IPv4 and IPv6 worlds, regardless of where they are or what type of device they're using," says Scott. "We can enforce the same context-aware policies on IPv6 that we've always had for remote users over IPv4, and from an IT perspective, it gives us a central point from which to control access policies."

Protects core network and applications

On its core (IPv4-based) network, the IT team has used previous versions of BIG-IP ASM to protect applications from layer 7 vulnerabilities such as DoS, DDoS, SQL injection, and cross-site scripting. With support for IPv6 in BIG-IP ASM 11.1, the IT team established BIG-IP ASM as the premier web application firewall solution across both its IPv4 and IPv6 networks. "BIG-IP ASM enables us to see the IP addresses of all devices, so we can detect security threats,

whether they're coming from IPv4 or IPv6 devices—it doesn't matter," says Scott. With that visibility, the IT team could also make F5's software download sites available on the IPv6 Internet. "Since we're able to see all source IP addresses, we can comply with regulatory and contractual obligations for secure downloading of BIG-IP software and cryptographic tools."

Enables secure collaboration among product development teams

In the past, F5's IT team had used the WAN optimization features of BIG-IP Edge Gateway for secure site-to-site SSL VPN communications between branch offices over IPv4; for IPsec communications, the team had evaluated third-party firewalls. However, now that BIG-IP Edge Gateway version 11.1 supports IPsec as well as IPv6, the team benefits from WAN optimization, IPsec, and IPv6 support on a single device, enabling it to eliminate other products.

"We're using our existing BIG-IP Edge Gateway devices at the edge of each network to establish an IPsec tunnel, for example, between product development and engineering teams in Seattle, Spokane, and San Jose," says Scott. "We can cross whatever network is between without any problems." Because BIG-IP Edge Gateway supports both IPsec and SSL VPN, the IT team has the flexibility to deploy whichever solution is most appropriate for each use case.

Reduces infrastructure costs

With enterprise demand for IPv6 circuits steadily increasing, more ISPs are beginning to offer larger IPv6 feeds. "Some ISPs are delivering an 'Ethernet handoff' now rather than the traditional serial interface to a third-party router," says Scott. That has enabled F5's IT team to eliminate third-party routers in its infrastructure, which cuts capital and operational costs, removes

a point of failure, and removes the security risk of a device that resides outside the firewall. "And now that we're using BIG-IP Edge Gateway devices to provide IPsec connectivity site to site, we've reduced the number of VPN concentrators."

Jon Caples, IT Dogfood Program Manager at F5 Networks, sums up the significance of the IT team's latest round of solutions for IPv6. "Many of our customers are facing these very issues. As customers begin to incorporate IPv6 support into their environments, they need solutions that will make the process as painless as possible. It's important that customers realize if they're building on a technology that is not native IPv6, they will have to do gymnastics to make it work well. But when they use a platform such as the BIG-IP system that is native IPv6, it will handle things automatically. It makes a huge difference in their ability to succeed."

F5 Networks, Inc.   401 Elliott Avenue West, Seattle, WA 98119   888-882-4447   www.f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com