



Basis-Informationen



F5 - Profil

F5 Networks ist das weltweit führende Unternehmen im Bereich Application Delivery Networking. Die von F5 Networks gebotenen Lösungen gewährleisten, dass Applikationen für jeden Anwender sicher, schnell und verfügbar sind. Indem das Netzwerk mit Intelligenz und Management-Funktionen zum Auslagern von Applikationen versehen und der Data Storage Layer verbessert wird, dehnt F5 die Leistung des Intelligent Networking auf alle Ebenen der Anwendungsübertragung aus. Die erweiterbare Architektur von F5 Networks integriert auf intelligente Weise die Anwendungsoptimierung, schützt sowohl die Anwendung als auch das Netzwerk und verbessert die Anwendungszuverlässigkeit – und dies alles auf einer universellen Plattform.

Zu den weltweit über 16.000 Organisationen und Service Providern von F5 Networks zählen unter anderem Bertelsmann, Citigroup, Commerzbank, Deutsche Bank, Ebay, Ericsson, Heise Verlag, Hypo-Vereinsbank, Microsoft, Siemens und T-Online.

Das Unternehmen mit Hauptsitz in Seattle, Washington, unterhält Niederlassungen weltweit und in allen europäischen Ländern. In Deutschland ist F5 mit der F5 Networks GmbH in München, Frankfurt, Köln und Berlin vertreten. Vom Logistic Center in Köln aus garantiert F5 Networks bundesweiten Hardware-Austausch. Zudem unterhält das Unternehmen eine Niederlassung im schweizerischen Baar.

Die rund 30 Mitarbeiter der deutschen Niederlassung erwirtschaften rund sechs bis acht Prozent des Gesamtumsatzes von F5. Künftig will das Unternehmen zehn Prozent erreichen. Deutschland ist für F5 neben Großbritannien wichtigster Markt in EMEA.

Entwicklungen

1996 brachte F5 die ersten lokalen Load Balancer auf den Markt, die seitdem kontinuierlich weiterentwickelt wurden. Es folgten eine Reihe innovativer Lösungen, die immer die aktuellen Anforderungen der Kunden erfüllen: Punkte wie Sicherheit und Performance sind hierbei ebenso wichtig wie Integrationsfähigkeit und einfache Administration. Um den ständig wachsenden Anforderungen des Marktes gerecht zu bleiben, investiert das Unternehmen bis zu 15 Prozent seines Umsatzes pro Jahr in die Forschung und Entwicklung. Hier werden bestehende Produktlinien im Sinne des Kunden verfeinert, aber auch zukunftsweisende Ideen Realität.

Markt und Geschäftsfelder

Drei Trends sind – unabhängig von der derzeitigen Wirtschaftssituation – ohne Zweifel für die nächsten Jahre ungebrochen und von steigender Bedeutung: Zum einen wird die Integration des Internets in die internen und externen Geschäftsprozesse vorangetrieben und hilft durch noch mehr Flexibilität, Kosten zu sparen. Zum anderen ist ein gesteigerter Sicherheitsbedarf gegen Angriffe, Spionage und Sabotage in den EDV-Abteilungen der Unternehmen Realität. Darüber hinaus sorgt die wachsende Anzahl der Internet-Nutzer für neue technische Herausforderungen und Lösungsansätze. Daraus ergibt sich eine immer stärkere Abhängigkeit vom Internet bzw. von Services, die über das Internet realisiert werden können.



Diese Trends ziehen einen steigenden Bedarf der Unternehmen an Hochverfügbarkeit bzw. Ausfallsicherheit der Services nach sich. Außerdem an

- Sicherheit, beispielsweise gegen Spionage und Sabotage
- schnellem Zugriff auf diese Services (Performance)
- kosteneffizienter Skalierbarkeit der Investitionen für zukünftige Anforderungen (Investitionsschutz) und
- einer einfacheren Handhabung der E-Business-Infrastruktur (Management).

Besonders interessant ist der Einsatz der F5 Lösungen für große Unternehmen – aber auch Service Provider und Carrier gehören zu den Kunden von F5. Die Traffic Management-Lösungen sind branchenübergreifend einsetzbar, da sie sowohl hohe Zugriffszahlen und Datenmengen auf einfache Weise managen als auch gesteigerten Sicherheitsbedürfnissen entsprechen. Die meiste Verbreitung haben die F5 Lösungen bisher in den Branchen Banken und Versicherungen, Medien und Industrie gefunden.

F5-Technologien im Überblick

F5 bietet umfassende Lösungen für das Traffic Management. Aufgabe des Traffic Managements ist es, IP-basierten Datenverkehr zu steuern und optimale Verfügbarkeit, Performance und Sicherheit von Netzwerk und Applikation zu erzielen. Die F5-Komponente fängt den gesamten IP-Verkehr ab, untersucht die Senderinformationen, kategorisiert diese nach Kriterien wie QoS (Quality of Service), Sicherheit, Applikationstyp oder sonstigen Geschäftsvorgaben und leitet die Anfragedaten schließlich an die optimale Quelle weiter. Neben Hochverfügbarkeit und Geschwindigkeit können bei der Auswahl auch die Funktionsfähigkeit angebundener Applikationen und die Sicherheit der Datenübertragung eine Rolle spielen. Intelligentes IP-Traffic Management umgeht fehlerhafte Netzkomponenten oder Service Provider, vermeidet so den Datenstau im Netzwerk und garantiert die Lieferung des gewünschten Contents.

iControl

F5 hat seine Software-Schnittstelle für die Applikationen anderer Hersteller geöffnet. iControl™ ist die branchenweit einzige Schnittstelle, die die Kommunikation und damit die Interaktion zwischen Netzwerk und Applikation ermöglicht. Von den F5-Komponenten generierte Daten und Statistiken über die Nutzung der Applikationen und Ressourcen können gelesen und beispielsweise zum Accounting und Billing genutzt werden. F5 kann über iControl auch eine Kommunikation zwischen Anwendung und Web Services herstellen.

iControl wird über SOAP/XML und CORBA Schnittstellen angesteuert und passt sich so unterschiedlichen Applikationserfordernissen an. Durch die Unterstützung von WSDL (Web Services Description Language) und SOAP/XML ermöglicht iControl die Aufzeichnung netzwerkkritischer Informationen und deren Kombination mit Daten über die Verfügbarkeit und Performance der Applikationen. Auf diese Weise können sowohl Applikations- als auch Netzwerkverhalten beeinflusst als auch Hochverfügbarkeit, beste Performance und Skalierbarkeit erzielt werden. Die iControl API unterstützt außerdem Microsoft.NET und J2EE Entwicklungsplattformen, so dass Entwickler die API durch bekannte Funktionen ergänzen und die Entwicklung beschleunigen können.



Integrierte SSL-Appliances

Der Industriestandard SSL (Secure Socket Layer) zur Ver- und Entschlüsselung sensibler Informationen ermöglicht den sicheren Datentransfer über das Internet. Die Funktionalität für das Ver- und Entschlüsseln der Daten kann zu Verzögerungen führen. F5 ist der einzige Anbieter mit einer in die Switches und Appliances integrierten und damit skalierbaren SSL-Lösung. Die SSL-Lösung von F5 ist darüber hinaus FIPS (Federal Information Processing Standard) Level 3 zertifiziert.

Application Traffic Management

Application Traffic Management ist eine Erweiterung des Traffic Managements, die neben der Geräte- auch die Applikationsebene (Microsoft, Siebel, Citrix, Oracle, BEA etc.) umfasst. Von den Vorteilen des Traffic Managements profitieren jetzt alle IP-basierten Applikationen und Web Services. Die Besonderheit liegt in der Tiefe, in der die Datenpakete analysiert werden können. So können z. B. normale Layer 4-7 Switches nur die Protokolle und Adressen lesen – während Application Traffic Management auch die Inhalte der Datenpakete (z. B. Session-Informationen der Applikationen) für die Traffic-Management-Entscheidung heranziehen kann.

Das neue BIG-IP-Konzept für das **Application Traffic Management** ruht auf zwei Säulen:

Universal Inspection Engine (UIE)

Sie dient der extrem schnellen Analyse der tief im Datenpaket enthaltenen Informationen. Damit können alle Informationen aus dem Datenpaket, etwa zu herstellerspezifischen Applikationsservern (BEA WebLogic, Microsoft, Oracle 9iAS etc.), XML-basierten Daten aus Web Services und mobilen Anwendungen, analysiert werden.

iRules

Mit diesem Tool können Administratoren vorab Regeln für die Behandlung der Datenflüsse – basierend auf der Analyse der UIE - einfacher als je zuvor definieren. Die Regeln lassen sich flexibel ändern oder einfach ergänzen. So wird eine signifikante Effizienzsteigerung beim Traffic Management erzielt: iRules erlaubt beispielsweise die Verteilung von „Read Only“- und „Read/Write“-Anfragen an Datenbankserver oder -segmente. Die Server-Performance wird auf diese Weise optimal für die jeweiligen Aufgaben genutzt.

F5 Produkte im Überblick

- **Traffic Management:**
 1. **BIG-IP® LTM:** Lokales Traffic Management plus SSL-Beschleunigung
 2. **BIG-IP® GTM:** Globales Traffic Management
 3. **BIG-IP® Link Controller:** Traffic Management von ISP und WAN

- **Sicherheit:**
 4. **FirePass®:** Sicherer SSL-VPN Applikationszugang
 5. **Application Security Manager/Modul:** Schützt Anwendungen vor Hackern und Day-Zero-Attacks
 6. **Message Security Modul:** Reputations-basierte Netzwerk-Sicherheit



- **Optimierung:**

7. **WANJet™:** WAN-Optimierung
8. **WebAccelerator™:** Beschleunigung von Web-Applikationen

- **Management:**

9. **Enterprise Manager:** Netzwerk Management

- **Storage:**

10. **F5-Acopia Data Solutions:** Technologie zur Datei-Virtualisierung



BIG-IP® Serie

Lokales Traffic Management plus SSL-Beschleunigung

Die BIG-IP Produktreihe wurde für das lokale Traffic Management konzipiert. F5 Networks präsentiert aktuell die Version 9.x von BIG-IP. Das Herzstück der neuen Generation ist TMOS – eine vereinheitlichte und schnelle Application Proxy-Architektur, die Unternehmen die absolute Flexibilität und Kontrolle über bestehende und künftige Anwendungen gibt. Anwendungssessions werden vollständig abgeschlossen, so dass Angriffe auf Netzwerkebene erst gar nicht bis zum Server vordringen.

Durch den Einsatz von BIG-IP erhalten die Kunden eine integrierte Lösung für alle IP-basierten Applikationen, die zentralisierte und vereinheitlichte Application Infrastructure Services bietet, wie Rate Shaping, Komprimierung, TCP-Optimierung, IPv6 Gateway, Load Balancing, Anwendungssicherheit, hoch performantes SSL und die vollständige Kontrolle über den gesamten Applikationsfluss. Durch die neue Architektur werden Performance-Einbußen oder höhere Wartezeiten ausgeschlossen.

Die modulare Architektur der BIG-IP-Lösung verkörpert ein neuartiges Design zur Überwachung, Kontrolle, Transformation, Programmierung und Skalierung der verschiedenen Services, die zur erfolgreichen Bereitstellung von Applikationen benötigt werden. Die Unified Application Infrastructure Services von BIG-IP erlauben Unternehmen, die benötigten Services effektiver zu kombinieren, zielgenauer einzurichten und zu erweitern, um die Wirksamkeit jeder eingesetzten Applikation zu steigern.

Durch die neuen Hardware-Plattformen wird die Leistung der BIG-IP-Application-Switches der nächsten Generation enorm gesteigert sowie Möglichkeiten geschaffen, sie einfacher zu managen, die Leistung auszuschöpfen und zu skalieren. Die IP-Application-Switches von F5 sind in der Lage, sowohl in Layer 4 als auch in Layer 7 extrem hohe Datenverkehrsbelastungen zu verarbeiten. Alle Plattformen bieten die Voraussetzungen für Multi-Boot Support, Upgrades im laufenden Betrieb, Lights-Out Management / Remote Boot und eine ausgezeichnete Systemausstattung. Zu den Modellen der neuen Plattform gehören auch die Application Switches 1500, 3400, 6400, 6800, 8400 und 8800.

Mit der neuen BIG-IP Generation wurde auch iControl™ wesentlich erweitert und optimiert, um so eine überlegene Performance und völlig neue Integrationsmöglichkeiten zu schaffen. iControl bietet ein vollständiges, event-basiertes API und ein Publish / Subscribe Modell, so dass BIG-IP Event Informationen zu jedem Gerät und jeder Anwendung weitergeleitet werden können. Um die Akzeptanz von v9 iControl zu erhöhen und eine schnelle Migration von existierenden Applikationen zu gewährleisten, bietet F5 eine Palette von Tools, wie z. B. einen Code Analyzer zur Unterstützung von Migration, umfangreiche Unterlagen und Beispiele, die Netzwerkadministratoren und Anwendungsentwicklern eine schnelle und komfortable Einführung von iControl ermöglichen.

SSL Acceleration

Die Funktionalität für SSL ist in den BIG-IP Controller integriert, die Performance (Transactions per Second) kann per Lizenz erhöht werden. Die F5 BIG-IP Appliances und Application Switches bieten so Traffic Management und SSL-Terminierung auf einer integrierten Plattform. Hardware, SSL-Entschlüsselung, Private Key und SSL-Zertifikaten-Management werden an zentraler Stelle konsolidiert und den Servern vorgeschaltet. Alle Server kommunizieren mit einer zentralen Stelle, die einen SSL-Schlüssel für die Kommunikation nach draußen vorhält. Auf diese Weise entfallen der Traffic für die einzelnen Authentifizierungs- und Encryption-Vorgänge sowie die zeit- und kostenaufwändigen Installationen von Zertifikaten und Hardware.



FirePass®

Sicherer Fernzugriff

FirePass ist eine Komponente, die den Anwendern einen sicheren Zugang zum Unternehmensnetzwerk über jeden Standard-Web-Browser ermöglicht. F5 Networks stellt mit seiner neuesten Version des FirePass® Controllers die branchenweit erste SSL-VPN Lösung zur Verfügung, die eine vollständige plattform-unabhängige Unterstützung bietet. Mit der erweiterten Unterstützung von Macintosh- und Linux-Clients und den nochmals erweiterten Sicherheitsfunktionen für Clients beim Zugriff über das Internet auf das Firmennetz und Anwendungen, liefert der FirePass Controller eine starke Lösung.

Mit den neuen Sicherheitsfunktionen werden die Unternehmensapplikationen und -daten noch besser geschützt. Die neue FirePass Version 6.x enthält Features wie bessere Client-Integrität, den „Protected Workspace“ sowie ein „Secure Virtual Keyboard“ für die Nutzung von Internet-Cafés, neue Virens Scanner und Schutz vor Attacken wie z. B. Cross-Site Scripting, Buffer Overflow, SQL Injection und vielen anderen.

Die wichtigsten FirePass Features im Überblick:

Verhindert die Manipulation von Web-Servern. Die Sicherheitsfeatures von FirePass Controller für Internetanwendungen blockieren Angriffe über die Anwendungsebene, wie z. B. Cross-Site Scripting, Buffer Overflow und SQL Injection durch die Überprüfung des gesamten Internetverkehrs über die FirePass.

Erhöhter Schutz vor infizierten Dateien. Ein Policy-basierter Virens Scanner bietet Kunden flexible Möglichkeiten und einen verbesserten Schutz. FirePass Controller ist in der Lage, Uploads aus dem Internet und aus Dateien zu scannen, indem es entweder einen integrierten oder einen externen Scanner via ICAP (Internet Content Adaptation Protocol) API benutzt. Infizierte Dateien werden am FirePass Gateway blockiert und können weder auf die Mailserver noch auf die Fileserver im Netzwerk gelangen.

Verbesserte Integrität des Clients und Quarantäne für unsichere Clients. Für eine sorgfältige Überprüfung der Integrität der Clients kann der FirePass Controller überprüfen, ob ein aktuelles McAfee Antivirus-Programm oder andere nutzerdefinierte Sicherheitsfeatures installiert und aktuell sind, bevor ihm eine vollständige Netzwerkverbindung gewährt wird. Kann ein Nutzer diese nicht vorweisen, kann eingeschränkter Zugriff auf ein besonderes Quarantäne-Netzwerksegment ermöglicht werden. Hier kann der Nutzer die Antivirus-Software oder Virendateien aktualisieren, um die Sicherheitsanforderungen des Unternehmens zu erfüllen.

Optimierte Sicherheit des Clients auf öffentlichen Web-Terminals (z. B. Kiosks oder Internet-Cafés). Der FirePass Controller beinhaltet eine neue Sicherheitsoption „Protected Workspace“, mit deren Hilfe Nutzer auf geschützte Arbeitsbereiche im Client-System (Windows XP/2000) wechseln können. Diese werden für jede Session neu angelegt. Befinden sie sich im gesicherten Arbeitsplatzmodus, können die Nutzer keine Dateien außerhalb des gesicherten Arbeitsbereiches auf dem Client-PC speichern. Die Ordner mit den Temporary Files werden mitsamt ihrem Inhalt nach jeder Session automatisch gelöscht. Das „Secure Virtual Keyboard“ des FirePass Controllers bietet zudem weitere verbesserte Sicherheitsfeatures beim Eingeben von Passwörtern. So werden zur Eingabe der Passwörter Mausclicks auf eine virtuelle Tastatur verlangt, welche die Aufzeichnung und den Diebstahl der Passwörter über „Spyware“ Software wirksam verhindert.

Schutz vor „back-door“-Angriffen. Sogenannte „back-door“-Angriffe nutzen die bestehende Verbindung in das Unternehmensnetz eines Clients, um sich über einen Angriff des



Clients darauf Zugriff zu verschaffen. Dies wird durch die „Split Tunneling“ Funktion der Fire-Pass verhindert, die über eine dynamische Firewall mit „Full Network Access“ verbundene Win2k/XP User zusätzlich schützt. Damit wird eine Nutzung des Clients als Zugang zum Tunnel sowie das versehentliche Senden von vertraulichen Daten in das öffentliche Internet verhindert.

Application Security Manager

Schützt Daten vor Hackern und Day-Zero-Angriffen

Application Security Manager ist eine auf der Anwendungsschicht arbeitende Sicherheitskomponente, die die Network Security von herkömmlichen Firewalls ergänzt. Mit dem Application Security Manager erhalten Unternehmen eine ausgezeichnete Lösung, um Anwendungen und Daten vor Hackern und anderen bösartigen Angriffen – inklusive Day-Zero-Angriffen – zu schützen, da das System nicht von Signaturen bekannter Angriffe abhängig ist. Damit präsentiert F5, führender Anbieter von Produkten für Application Traffic Management und Application Security, einmal mehr eine zukunftsweisende Innovation auf dem Security-Markt.

F5's Application Security Manager folgt dem Prinzip der positiven Sicherheit und steht damit im Gegensatz zu anderen Sicherheitseinrichtungen im Netzwerk. Denn Netzwerk-Firewalls, Intrusion-Detection-Systeme (IDS) und andere punktuelle Sicherheitssysteme arbeiten mit einer Logik der negativen Sicherheit und bieten daher nur vor bereits bekannten Sicherheitsbedrohungen Schutz. Der Application Security Manager gewährleistet hingegen, dass die Anwender unbeschränkten, sicheren Zugriff auf alle benötigten Informationen haben und verhindert gleichzeitig, dass jemand die Anwendungen selbst manipulieren kann. Die Software des Application Security Manager und die 4100 Hardware-Plattform sind entscheidende Komponenten von F5's Strategie für Sicherheitsprodukte zum Schutz der Applikationen unabhängig von der Netzwerk-Infrastruktur.

Die neue Plattform der 4100-Serie

Eine Schlüssel-Komponente des Application Security Managers ist F5's neue Hardware-Plattform aus der 4100-Serie. Zuverlässig und einfach in der Handhabung, bietet sie Sicherheitsfunktionen und Performance für höchste Ansprüche. Die 4100 Plattform ist das erste System auf dem Markt, das für die SSL-Beschleunigung nicht nur den Verbindungsauf- und abbau optimiert, sondern mit Hilfe einer speziellen Hardware die Ver- und Entschlüsselungen (3DES/AES bulk crypto) des laufenden Datentransfers vornehmen kann.

Zur Verteidigung gegen gezielte Angriffe durch Hacker validiert das Application Flow Model (AFM) vom Application Security Manager jede Transaktion auf der Basis von User Session, Eingaben des Anwenders und zurückgegebenen Inhalten. Bei diesem Hochsicherheitsverfahren werden nur solche Anwendungstransaktionen zugelassen, die zuvor als gültig erkannt wurden, alle anderen werden unterbunden. Zusätzlich bietet der Application Security Manager ein leicht zu handhabendes, Anwenderrollen-basiertes Verwaltungsportal für die Netzwerk- und Anwendungsadministration, das mit Remote Device Configuration, Visual Application Security Policy Management, Full Logging, Auditing und Reporting ausgestattet ist.



BIG-IP® GTM

Globales Traffic Management

Für das globale Traffic Management entwickelte F5 den Global Traffic Manager. Dieser steuert das Load Balancing geographisch verteilter Internet-Sites und Rechenzentren. Fällt ein Standort aus, werden Anfragen an das verfügbare Datacenter geleitet. Ebenso können Entscheidungen nach Performance, User-Nähe oder auch zeitgebunden getroffen werden: Durch die Zeitverschiebung ist es sinnvoll Rechenzentren anderer Länder anzusteuern, da der IP-Traffic nachts in der Regel sehr gering ist. Der Kunde kann die Regeln zur Verteilung des Datenverkehrs selbst definieren.

Enterprise Manager

Geringere Kosten und zentralisierte Verwaltung für mehrfache F5 Geräte

F5's Appliance Enterprise Manager versetzt Unternehmen in die Lage, F5 Geräte die in das Netzwerk zu integrieren, zentral zu identifizieren und zu warten. Mit Hilfe des Enterprise Managers ist es möglich:

- die Konfigurationen der Geräte für die Notfallplanung zu archivieren und zu sichern.
- neue Geräte von einem zentralen Ort aus zu konfigurieren, ohne an den einzelnen Geräten manuell Einstellungen vornehmen zu müssen.
- Personalkosten für die Verwaltung mehrfacher F5 Geräte zu reduzieren.
- einfach und schnell neue Software-Versionen und Sicherheits-Patches auszurollen.

Der Enterprise Manager erlaubt es auch, per Knopfdruck neue Software-Versionen und Hot Fixes auf mehrfache Geräte gleichzeitig aufzuspielen. Beim Aufspielen der neuen Software-Versionen bewahrt er die bestehenden Konfigurationen und Lizenzierungen der Geräte, so dass man bei Upgrades keine wichtigen Informationen verliert. Der Status der Upgrade-Installation wird deutlich angezeigt, die erfolgreiche Ausführung wird per E-Mail bestätigt.

Das Leistungsportfolio des Enterprise Managers ermöglicht darüber hinaus Templates zu erstellen, die Geräte-Profile, Konfigurations-Einstellungen, iRule Definitionen und vieles andere enthalten. Die Templates werden erstellt, indem man einfach ein vorhandenes Gerät ausliest oder aber direkt ein eigenes erstellt. Einmal eingerichtet, können mehrere Templates in dem Enterprise Manager gespeichert und verwaltet werden. Die Templates des Enterprise Managers gewährleisten, dass Ihre Kunden durchgehenden Service erhalten, während Sie Ihr Netzwerk skalieren, um Wachstum zu bewältigen.

Sicherheitsmodul (ASM)

Enterprise-class Sicherheit auf der Anwendungsebene

BIG-IP hat ein neues Sicherheitsmodul (ASM), das auf der Technologie von F5's Anwendungs-Firewall TrafficShield basiert. Das Modul bietet enterprise-class Sicherheit auf der Anwendungsebene, die vollkommen in den BIG-IP integriert ist und auf der TMOS-Architektur, der Basis für Anwendungsnetzwerke, aufbaut.

Das Sicherheitsmodul kombiniert umfangreiche Funktionen für die Sicherheit, Beschleunigung und Zuverlässigkeit von Anwendungen in einem einzigen, richtlinien-basierten Framework. Damit bietet F5 seinen Kunden als erstes Unternehmen eine kosteneffiziente, leistungsfähige und vereinheitlichte Plattform für die erfolgreiche Bereitstellung von Anwendungen.

Das BIG-IP ASM bietet Web-Anwendungen mehr pro-aktiven Schutz als traditionelle Lösungen auf der Netzwerk-Schicht. Deshalb setzt der ASM die Anwendungs- und Netzwerkservices, die zu seinem TMOS-Betriebssystem gehören, wirksam ein und bildet so die umfas-



sendste Netzwerklösung zur Bereitstellung von Anwendungen, die auf dem Markt erhältlich ist. Damit bekommen Unternehmen eine bessere Netzwerk-Alternative, die die Anzahl der Geräte reduziert, Wartungs- und Verwaltungskosten senkt und noch mehr pro-aktiven Schutz bietet, während gleichzeitig eine außergewöhnlich gute Performance gewährleistet ist.

BIG-IP Link Controller

WAN Link Traffic Management der nächsten Generation für höchste Verbindungsstabilität und Verfügbarkeit

Der BIG-IP Link Controller überwacht nahtlos die Verfügbarkeit und Performance von mehrfachen WAN ISP Verbindungen, um bidirektionalen Traffic Flow zu einer Webseite intelligent zu verwalten. Auf diese Weise wird ein fehlertoleranter und optimierter Internet-Zugriff gewährleistet.

Der BIG-IP Link Controller setzt F5's TMOS-Architektur optimal ein und bietet eine verbesserte Verbindungsstabilität und hohe Verfügbarkeit, außerdem eine flexible und leistungsstarke Zustandskontrolle, umfassende Sicherheit und eine hohe Nutzerfreundlichkeit.

Der Link Controller baut zuverlässige WAN-Verbindungen für eine geschäftstaugliche Internet-Anbindung auf und nutzt dank Rate Shaping effizient die Bandbreiten von WAN-Verbindungen. Zudem reduziert diese Technologie den Verbrauch von Bandbreiten für WAN-Verbindungen durch den Einsatz von Komprimierung und verbessert durch Optimierungen von TCP/IP mit Hilfe von TCP Express die Performance spürbar. Darüber hinaus gewährleistet der Link Controller, dass der Traffic über die beste verfügbare Verbindung und den besten ISP geleitet wird, um höchstmögliche Geschwindigkeit und Quality of Service zu erreichen. Der ROI der Internet-Anbindung wird durch die Bündelung kostengünstiger Verbindung reduziert.

WanJet,

Performance wie im LAN

WANJet ist die Hardware-Lösung von F5, mit der Anwendungen im WAN eine Performance erreichen, die mit der im LAN vergleichbar ist. WANJet beschleunigt z. B. die Übertragung von Dateien, E-Mail-Programmen, Client-Server-Anwendungen oder Datenreplikationen. Ergebnis ist eine zuverlässige, schnelle Performance für alle WAN-Benutzer. In Rechenzentren wird WANJet 500 eingesetzt, der sich durch seine Fehlertoleranz, Skalierbarkeit und eine Performance von bis zu 400 Mbit/s auszeichnet. Beim Einsatz in Filialen wird WANJet 200 installiert, der ebenfalls Funktionen zur Fehlertoleranz, einen geräuscharmen Betrieb sowie eine Performance von bis zu 2 Mbit/s bietet.

Die anpassungsfähige TCP-Optimierung von WANJet (mit Application Awareness auf Session-Ebene, beständigen Tunnels, selektiver Bestätigung, Fehlerkorrektur und optimierten TCP-Fenstern) überwindet protokollbedingte Herausforderungen und nutzt die verfügbare Kapazität vollständig aus. Dadurch kann sich WANJet in Echtzeit an die Latenz, den Paketverlust und die Datenstauereigenschaften von WAN-Links anpassen und den gesamten Anwendungsdatenverkehr beschleunigen.

WANJet bietet eine Site-to-Site-Verschlüsselung mit SSL, das heißt: Schnelligkeit bei gleichzeitiger Sicherheit. Der Anwendungsdatenverkehr wird in Hochgeschwindigkeit abgewickelt – in jedem WAN und mit vollständigem Datenschutz. Die Benutzer profitieren von der Transparenz und Geschwindigkeit, die IT-Mitarbeiter können sicher sein, dass die Unternehmensdaten geschützt sind. Die Unternehmensleitung kann sich darauf verlassen, dass Bestimmungen wie Sarbanes-Oxley eingehalten werden.



WebAccelerator

Hohe Geschwindigkeit für Web-Applikationen

Der WebAccelerator ist für Unternehmen gedacht, die eine hohe Geschwindigkeit für ihre Web-Applikationen benötigen. Erhältlich ist er auch auf F5's fortschrittlicher TMOS-Architektur und wird als ein Zusatzmodul für die BIG-IP 6400, 6800, 8400 und 8800 Plattform geliefert. Durch die Integration in TMOS übernimmt der WebAccelerator leistungsstarke Funktionen wie iRules, QoS, Paket-Filter und TCP Express. Die leistungsstarke WebAccelerator 4500 Plattform steht für große Leistungsfähigkeit und zeichnet sich durch eine hohe Verfügbarkeit und einfache Bedienung aus. Darüber hinaus gewährleistet sie neben einer langen Lebensdauer über einen niedrigen TCO.

Dank F5's einzigartigen geprüften Beschleunigungsrichtlinien für Web-Applikationen und den intelligenten Browser-Referenz-Technologien verfügt der WebAccelerator über die in der Branche fortschrittlichsten Fähigkeit der Web-Applikations-Beschleunigung. Diese Richtlinien bieten spezielle Konfigurationsmöglichkeiten, die von Microsoft, Siebel, Oracle und Plumtree/BEA AquaLogic zertifiziert und getestet wurden und von denen bewiesen wurde, dass sie auf den genannten Plattformen effektiv funktionieren.

Zudem können die Richtlinien als eingebaute Templates fungieren und ermöglichen eine schnelle Anpassung an spezifische Web-Applikationen. Die intelligenten Browser-Referenz-Funktionalitäten des WebAccelerator räumen Probleme aus dem Weg, die sich auf die Performance der Web-Applikationen negativ auswirken, wie z. B. WAN-Latenz und negatives browser-seitiges Verhalten. Im Gegensatz zu anderen Lösungen bietet die intelligente Browser-Referenz des WebAccelerator einen vollkommen client-losen Ansatz und verbessert die Anwendungsperformance um das Drei- bis Zehnfache.

F5 Acopia Data Solutions

Intelligente Technologie zur Datei-Virtualisierung

Die F5 Acopia Data Solutions optimieren die Dateispeicherungsebene, indem sie Mitarbeitern in Unternehmen unabhängig von ihrem jeweiligen Standort einen schnelleren und sichereren Zugriff auf Applikationen ermöglichen. Die Intelligente Datei-Virtualisierung ermöglicht ein besseres Informationsmanagement und verhindert ein Ausufernd der Betriebskosten.

Die F5 Acopia-Produktfamilie besteht aus den fest konfigurierten Systemen ARX500 und ARX1000 sowie der chassisbasierten Lösung ARX6000. Alle Plattformen unterstützen den gleichen Bestand an Software-Services und Funktionalität und zielen lediglich auf unterschiedliche Skalierungs- und Kapazitätsanforderungen der Kundenumgebung. Die mit drei verschiedenen Plattformen verfügbaren ARX-Systeme basieren alle auf dem Netzwerk-Betriebssystem FreedomFabric™, unterscheiden sich aber bezüglich ihrer Leistungsfähigkeit und ihres Umfangs, wobei die Skala vom Low-End-Produkt ARX500 bis zur High-End-Lösung ARX6000 reicht. ARX500 stellt als ‚Thin Server‘ Switch das Einstiegsmodell für Abteilungen oder Regionalniederlassungen dar. Die Mittelklasse verkörpert der Switch ARX1000 für Unternehmen und regionale Datacenter. Mit einem hohen Performance- und Verfügbarkeitsniveau erfüllt der Switch ARX6000, ausgelegt für Unternehmensrechenzentren, hohe Ansprüchen an die Performance und Skalierbarkeit.

Die ARX-Produkte automatisieren das Verlagern von Dateien zwischen heterogenen Dateispeicher-Geräten – ohne Einfluss auf den Zugriff und ohne dass ein Rekonfigurieren des Clients erforderlich ist. Unternehmen können während des laufenden Geschäftsbetriebs



nahtlose Hard- und Software-Upgrades an den Dateispeicher-Plattformen vornehmen. Auch Storage-Konsolidierungen und sogar ein Wechsel zu einem anderen Anbieter sind möglich. F5 Acopia fungiert als Front-End für NAS Devices und beliebige Dateispeicher-Ressourcen, dient dabei als File Server Proxy (CIFS, NFS) und unterstützt Virtualisierungs- und intelligente Datenmanagement-Policys für die gesamte Storage-Umgebung eines Unternehmens. Es bleibt den Unternehmen somit erspart, einen Komplettaustausch ihrer Hardware vorzunehmen, existierende Dateisysteme zu ersetzen oder im gesamten Unternehmen Software-Agenten zu laden, damit die Vorteile der Virtualisierung genutzt werden können.



Partner

F5 pflegt zahlreiche Partnerschaften mit marktführenden Unternehmen:

- OEM Partner: Dell, Nokia, Ericsson
- Technologiepartnerschaften: Nokia, Network Appliance
- iControl Partner: BEA, Siebel, Citrix, Microsoft, Oracle, Tivoli, Dell, HP

F5 Partnerprogramm

Das F5 Partnerprogramm bietet umfangreiche Leistungen für die Zusammenarbeit sowohl mit Distributoren und Resellern als auch mit strategischen Partnern. Ziel des Programms ist, jedem Partner von F5 die notwendige Unterstützung zu gewähren und die geeigneten Tools, Trainings und Services bereitzustellen, um den geschäftlichen Erfolg der Partner zu sichern und zu steigern. Partner des F5 Advantage Programs sind dazu berechtigt, F5 Produkte zu verkaufen, zu installieren, zu konfigurieren und Support-Leistungen bereitzustellen. Sie verpflichten sich zur Teilnahme an den spezifischen Fortbildungs- und Trainingsmaßnahmen. Des Weiteren stellt F5 den Distributoren und Resellern Sales Trainings, Tools und Ressourcen zur Verfügung, um ihr Geschäft aufzubauen und eine starke Kundenbasis zu entwickeln. In dem Maße wie das Engagement der Partner gegenüber F5 wächst, nimmt für sie auch der Nutzen des Programms zu.

F5 EMEA Support

Im EMEA Support Center in London kümmern sich Netzwerkspezialisten, Berater und Schulungspersonal um die Belange autorisierter Partner in Deutschland, Frankreich, Irland, Italien, Spanien, Großbritannien, Skandinavien und den Benelux-Staaten. Neben der umfangreichen Online-Datenbank „Ask F5“ (www.F5.com) bietet das Support Center auch deutschsprachige Unterstützung bei technischen Fragen. Speziell ausgebildete Fachkräfte stehen den Partnern telefonisch zur Verfügung und beraten persönlich bei komplexen Lösungsszenarien.



Analysten über F5

Traffic Management / Dell'Oro Group

Laut Marktführungsinstitut Dell'Oro Group rangiert F5 auf dem Traffic Management-Markt – Appliances und Layer 4-7 Switches – mit 38% Marktanteil weltweit an erster Position.

Traffic Management Appliances / Dell'Oro Group

Im Bereich Traffic Management Appliances ist F5 – so die Dell'Oro Group - mit 68% Marktanteil weltweit die Nummer eins.

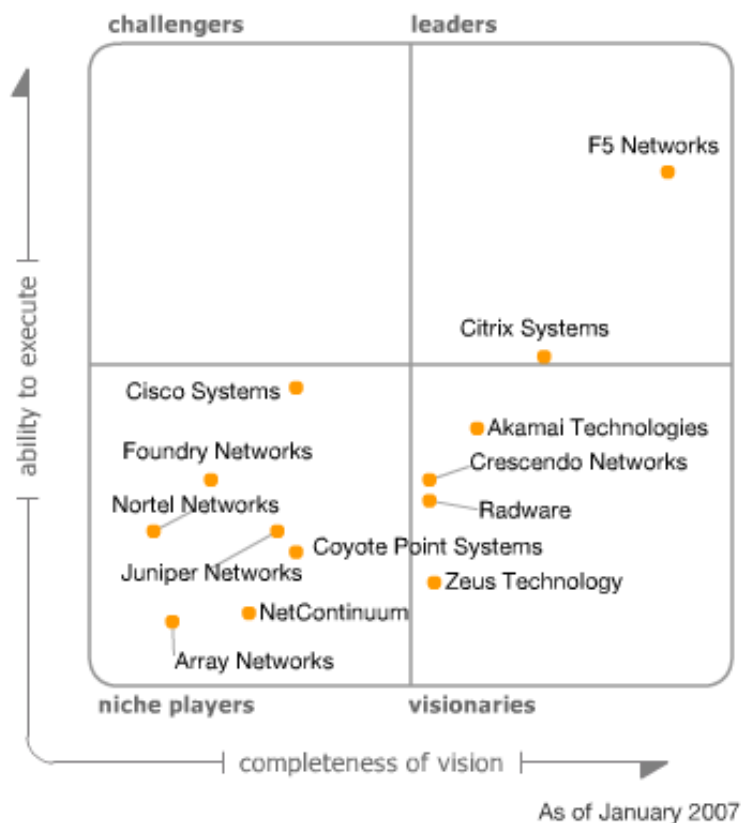
SSL-Hardware / Infonetics Research

Infonetics Research bestätigte in einer Studie vom Mai 2003 F5's Marktführerschaft im Bereich Layer 4-7 Switch/Load Balancer mit SSL (79% Marktanteil)

Web Infrastructure Optimization Devices / Gartner Group

Die Auguren der Gartner Group positionierten F5 in dem aktuellen magischen Quadranten ihrer Web Infrastructure Optimization Studie im Januar 2005 als klaren Marktführer.

Gartner Magic Quadrant Bereich Application Delivery Produkte 2007





Management

Martin Räder

Regional Director für Central und Eastern Europe

Martin Räder lenkt als Regional Director seit Sommer 2007 die Geschicke von F5 für Central und Eastern Europe. Der studierte Informatiker bringt dabei seine umfassenden Erfahrungen, die er in über 20 Jahren Berufspraxis in der IT-Branche gesammelt hat, ein. Seinen Fokus hat er dabei auf die Bereiche Management, Vertrieb und Marketing aber auch auf das Business Development gelegt. Bevor Martin Räder bei F5 Networks tätig wurde, verantwortete er als Regional Director sechs Jahre bei der Firma NetIQ die Länder Zentral- und Ost-Europas. Dem ging seine vierjährige Tätigkeit als Geschäftsführer der Interlink Deutschland GmbH und als Director Business Development der Interlink Computer Sciences in Fremont, Kalifornien, voraus. Zu Beginn seiner beruflichen Laufbahn war Räder in Management Positionen bei der Nixdorf Computer AG, als auch bei der Schneider Rundfunkwerke AG, in leitender Funktion tätig.

John McAdam

President, Chief Executive Officer und Director

John McAdam ist seit Juli 2000 President, Chief Executive Officer und Director von F5, Inc. Bevor er zu F5 stieß, war McAdam General Manager für das Web Server Sales Business bei IBM. Von Januar 1995 bis August 1999 leitete John McAdam Sequent Computer Systems, Inc. als Chief Operating Officer. Sequent Computer Systems, Hersteller von Offenen High-End Systemen, wurde im September 1999 an IBM verkauft. John McAdam hält einen Bachelor of Science in Computer Science der University of Glasgow, Schottland.

Ansprechpartner für Journalisten

F5 GmbH
Claudia Kraus
Einsteinring 35
D-85609 München-Dornach
Tel.: +49 (0)89 94 383 220
Fax: +49 (0)89 94 383 111
E-Mail: c.kraus@f5.com
Internet <http://www.f5networks.de>

HBI GmbH Int. PR& MarCom
Corinna Voss, Antonia Contato
Stefan-George-Ring 2
D-81929 München
Tel: +49 (0)89 99 388 7 -0
Fax: +49 (0)89 93 02 445
E-Mail Antonia_contato@hbi.de
Internet <http://www.hbi.de>