

Forrester Consulting

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE

July 2007

Moving IT From Application Deployment To Application Delivery

A Guide to Application Delivery for
Network Architects

Spotlight: Web Applications and WANs
(Part two in a series of four)

*A commissioned study conducted by Forrester Consulting on
behalf of Citrix Systems*

FORRESTER®

FORRESTER®

Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617/613-6000 • Fax: +1 617/613-5000 • www.forrester.com

Table Of Contents

Application Delivery Definition	3
Executive Summary	3
From Packets To Policy: Why Network Architects Must Focus On Applications.....	3
Network Architecture Decision-Makers Prioritize Application Security And Business Continuity Initiatives.....	4
How Application Delivery Helps Network Architects	5
Application Delivery Shifts The Emphasis From Deployment To Delivery	6
Application Delivery Infrastructure Addresses Emerging Network Architecture Requirements.....	6
The Dos And Don'ts Of Application Delivery	8
Conclusion	9
Appendix.....	9
Research Methodology.....	9

© 2007, Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, WholeView 2, Technographics, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Forrester clients may make one attributed copy or slide of each figure contained herein. Additional reproduction is strictly prohibited. For additional reproduction rights and usage information, go to www.forrester.com. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Application Delivery Definition

"Application Delivery" is the process of getting applications from the data center to the user as efficiently as possible. "Application Delivery Infrastructure" refers to the technology components that enable this efficiency across any network. A comprehensive application delivery infrastructure includes technologies that improve performance, availability, and security without compromising flexibility. Specifically, this includes components like application accelerators, desktop and application virtualization, application firewalls, secure remote access, WAN optimization, and performance monitoring.

Executive Summary

The network architect role has changed dramatically in the last few years. Five years ago, most network architects focused on capacity planning and network topology, and measured their success with factors like low latency and high throughput. Today is a different story. These skills are still required, but network architects are now held accountable for application — not packet — metrics. In fact, we've found that application availability, application security, and application performance now represent the top three network architecture concerns.

To address these emerging application requirements, Forrester recommends a twofold approach:

- **Empower network architects to influence application strategies.** The goal is simple: allow any user to connect to any app with a great user experience and the right level of security. But most organizations don't think to include network teams in this strategy upfront, despite the fact that the network is the "glue" between users and applications. By including network architects early and often, an IT organization can more easily respond to lines of business and application owners.
- **Invest in an application delivery infrastructure.** Network architects today are faced with emerging requirements around application-layer security, disaster recovery preparedness, access control, and application performance. By investing in the application delivery infrastructure, network architects have a single policy-driven infrastructure that provides the necessary control, optimization, and visibility needed to address these concerns.

From Packets To Policy: Why Network Architects Must Focus On Applications

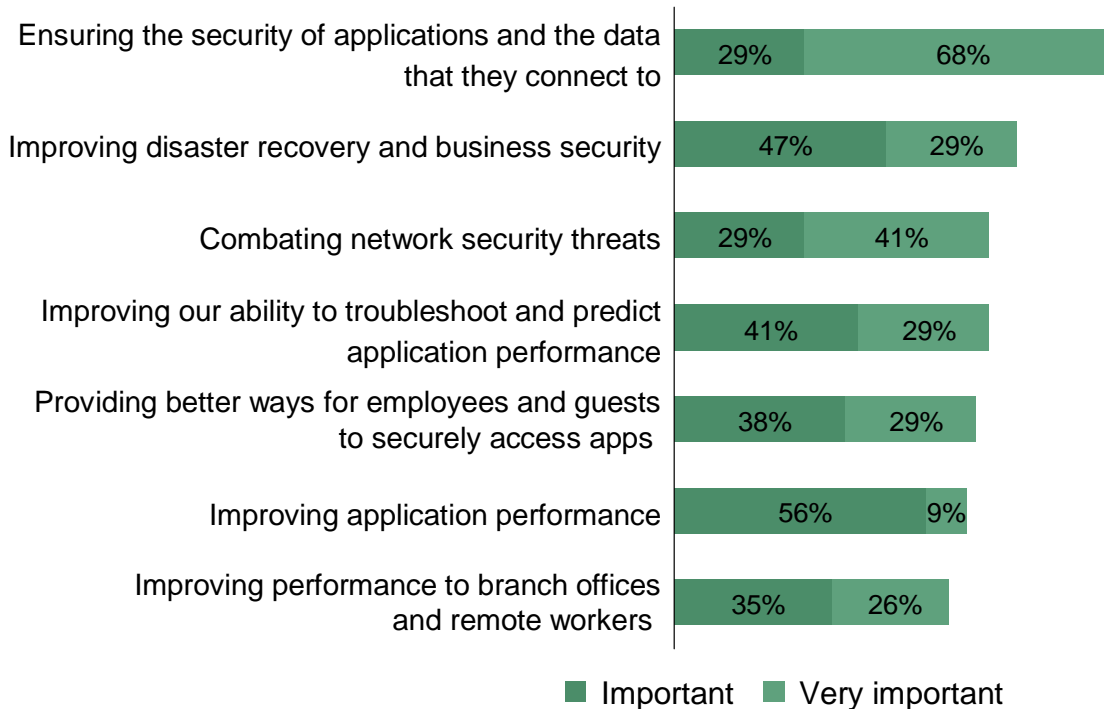
As part of a study commissioned by Citrix, Forrester Consulting recently surveyed IT decision-makers in charge of network architecture and found that a surprising 30% of their time is spent on application-oriented issues, a significant increase over previous years. We also found that the two lowest priorities for these network architects were reducing network infrastructure lifecycles and decreasing support costs — two functions that their network operations colleagues prioritize. Why is this? Because network architecture isn't about packets anymore; it's about policies. Policies for users and applications — the two things networks are intended to connect — translate the binary world of the network into more relevant business objectives for application security, performance, and availability. As a result, today's network architects must stay on top of evolving application frameworks. In fact, 56% of these network decision-makers agreed that emerging application trends like services-oriented architecture (SOA), Web services, and Web 2.0 would have a major impact on network infrastructure.

Network Architecture Decision-Makers Prioritize Application Security And Business Continuity Initiatives

The changing business climate requires more responsive networks. In turn, as network architects evolve to become more responsive — and adopt higher-levels of application responsibility — they need to address new requirements. Today's network architects must (see Figure1):

- **Secure applications and combat evolving network threats.** In today's environments, most security threats are sophisticated, focused attacks with business data as the primary target. Since applications are the main conduit to sensitive data, they are increasingly the focus of these attacks. The maturation of security technologies means architects must design a secure network fabric to protect sensitive data and maintain network uptime. As a result, two of the top three concerns facing today's network architects are security related. An overwhelming 97% of network architects listed application security to be the top 2007 priority; and not far behind at No. 3 on the list is combating network security threats.
- **Improve business continuity capabilities.** The increasing threat of natural and manmade disasters means IT must be prepared to extend application access to users regardless of location. Moreover, it further stresses the needed for an "always on, always available" network. So it's no surprise that disaster recovery and business continuity is the No. 2 network architecture priority with 76% of respondents listing it as a 2007 priority.
- **Focus on application performance, especially for Web apps.** For most organizations, the network is guilty until proven innocent for performance issues. This is exacerbated by the migration of client/server applications to the Web, where network infrastructure plays an increased role in connecting and protecting users. Simply "throwing bandwidth at it" won't address the underlying application response times. In fact, 71% and 65% of network architects cited improving application performance troubleshooting and improving overall application performance as important 2007 initiatives, respectively.
- **Make applications easily accessible from any location.** Today's enterprises are expected to do business in a flat world. But it's a nonstop challenge to deliver applications to an increasingly mobile set of users in branch offices, home offices, and on the road. Moreover, these aren't just your employees. Customers, suppliers, and partners are all critical user constituencies. In fact, nearly two thirds of network architects listed secure access and improving performance as 2007 priorities.

Figure 1: Security And Disaster Recovery Top The 2007 Network Architecture Priority List
“How important are the following IT priorities for 2007?”



Base: 34 network architecture decision-makers

Source: A phone survey of 153 IT decision-makers and influencers across North America, Europe, and Asia-Pacific in March 2007 commissioned by Citrix and conducted by Forrester Consulting.

How Application Delivery Helps Network Architects

Does this sound familiar? You just spent tens of millions of dollars on a new Web-based version of your ERP system, but it's a little sluggish. Your users are complaining about a lack of productivity, and partners aren't adopting the new portal because it takes five minutes to log in. It's got to be a network problem, right? Unfortunately, it's not that simple; application performance is a complicated matter. Data bases, middleware platforms, servers, storage, and networks are all critical components.

However, there's an emerging technology solution that helps. Forrester refers to it as application delivery infrastructure. We define this as:

Technologies that streamline the connection of any user to any application by minimizing deployment burdens, reducing management costs, optimizing performance, and increasing security.

Application Delivery Shifts The Emphasis From Deployment To Delivery

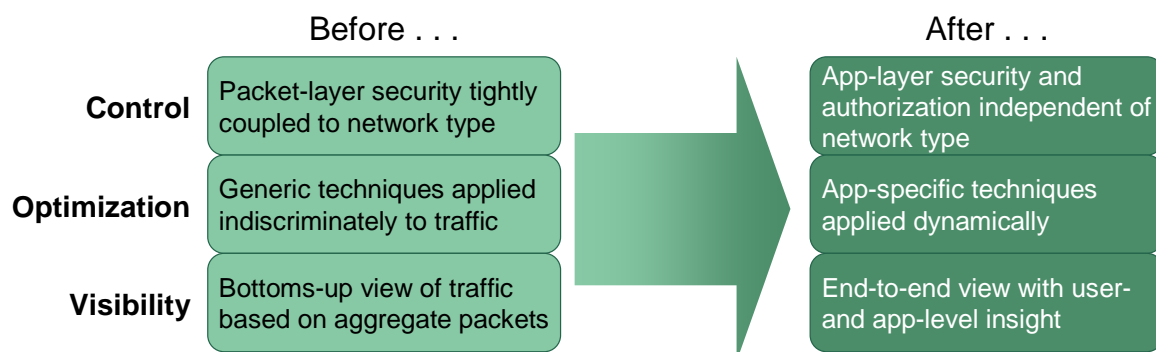
Application delivery *isn't* about throwing more bandwidth at the problem. Instead it's a combination of solutions that bridges that gap between the network's packet-processing layers — Layers 1 through 3 in the traditional OSI stack — and application layers. It's the platform that provides the necessary abstraction layer to make the shift from packets to policy.

Application delivery infrastructure means network groups can become less reactionary and take proactive measures to secure and accelerate applications. It breaks the traditional cycle of incremental improvements like bandwidth upgrades and provides a single pane of glass to manage all aspects of application traffic. Put simply, application delivery helps network architects shift the emphasis from application deployment to application delivery.

From a network perspective, application delivery infrastructure provides (see Figure 2):

- **Control.** Emerging security, access, and compliance issues means network architects need control. Application delivery provides the proper application-level authentication, authorization, and mitigation of potential risks.
- **Optimization.** Increasingly complex applications mean network architects must guarantee performance across any network medium — wired, wireless, and remote. Optimization techniques provide acceleration and application traffic management to avoid bottlenecks.
- **Visibility.** Application monitoring tools provide end-to-end insight. The result? Network managers have a more relevant view of the end user experience across their environment, not just the performance of protocols and packets; as a result, they can accurately identify, troubleshoot, and apply the necessary control and optimization policies.

Figure 2: Application Delivery Provides Better Control, Optimization, And Visibility



Source: A study commissioned by Citrix Systems and conducted by Forrester Consulting.

Application Delivery Infrastructure Addresses Emerging Network Architecture Requirements

Focusing on application delivery infrastructure allows IT organizations to transform the network from a basic transport system to an on-demand delivery system (see Figure 3). For a network architect, it means cost effectively:

- **Mitigating evolving application threats and extending secure application access.** Networks have become cluttered. Rather than throwing more security widgets at the problem, network architects need to fundamentally rethink the way they protect users and data. Specifically, application delivery infrastructure provides application-savvy firewalls and secure-access technology like SSL VPNs, some of which are now integrated into comprehensive application accelerators and switches that make it easier to centrally manage application policy. Thus, protection occurs at the application layer of the network. Should you replace network security? No, but in a layered defense model, application delivery can mitigate evolving threats disguised on port 443 — which your network firewall would ignore. Furthermore, it provides the authentication, authorization, and access control to safely extend your application resources to non-corporate users.
- **Increasing business continuity preparedness.** Network architects can avoid costly downtime with global load balancing of mission critical applications. If a disaster strikes a given area, then the application delivery systems can seamlessly redirect users to any global data center. Moreover, WAN optimization technologies accelerate data replication and application synchronization among all your global points of presence. And finally, SSL VPNs provide a clientless remote access so you can guarantee workforce continuity regardless of the users' location.
- **Monitoring the end-to-end application experience.** It's difficult to tease out nuances like which application consumes the most bandwidth and to which locations; or what the application response time is relative to a given user. Application delivery infrastructure overlays end-to-end insight independent of network medium. It provides a twofold capability for monitoring and reporting tools that measure: 1) end-user experience and 2) application-specific flows. This not only increases visibility, but provides the relevant information needed to reduce the operational costs of troubleshooting and maintaining application performance. Most importantly, it equips the network staff to accurately measure and maintain SLAs as evolving Web services and Web 2.0 applications, which introduce new protocols and traffic types.
- **Improving application performance to all users.** Network architects must still extend application connectivity to users that are leaving corporate headquarters to work remotely. Application delivery infrastructure provides a wide range of optimization techniques like caching, compression, protocol acceleration, offload, and traffic management to iron out performance wrinkles. From a technology perspective, this includes 1) next-generation load balancers with acceleration, which improves application performance to users coming in from the Web; and 2) WAN optimization appliances, which improves application performance for users connecting from a branch office.

Figure 3: Application Delivery Addresses Emerging Network Architecture Requirements

Emerging requirement	How application delivery helps
Threats are becoming increasingly sophisticated.	Application firewalls expand security technologies to the application layer.
More partners, suppliers, and customers need access to sensitive apps and data.	SSL VPNs are gateways that extend secure app access to guests and mobile users.
New business continuity plans require faster time to recovery from disasters.	Next-gen load balancers provide global failover of apps and quick recover times.
Networking staff can't accurately troubleshoot and monitor app traffic.	Monitoring tools provide end-to-end visibility of user and application transactions.
Increasing remote and branch office workers creates network bottlenecks.	WAN optimization accelerates application traffic over the internet and WAN.

Source: A study commissioned by Citrix Systems and conducted by Forrester Consulting.

The Dos And Don'ts Of Application Delivery

It's important to make sure you have a consistent architectural approach so you can ensure end-to-end application control, optimization, and visibility. We recommend that you:

- **Do include network architects early and often.** Only 21% of network architects strongly agreed that the networking team is engaged early in most application rollouts and works closely with application groups. This lack of collaboration will drive the biggest wedge into any application delivery strategy. Even if you don't consider your network to be a strategic asset, you still need to empower your network architects to get involved in application strategies. Application delivery infrastructure is the relevant platform to start this collaboration. Be careful about giving this role to network operations leaders, though. While they clearly need to be involved, network operations teams tend to be very focused on maximizing the operational efficiencies of the transport network and generally have a hard time seeing the broader importance of applications and their impact on network architectures.
- **Do implement the underpinning technologies . . .** Most companies have already started down the application delivery path. In fact, 62% of network architects cited that even emerging technologies like SSL VPN and WAN optimization are already important parts of their architecture. These newer technologies provide the foundation for moving applications from a traditional deployment to a more flexible delivery model.
- **. . . But don't just default to your standard networking vendor.** It's important to distinguish between your networking vendors: those that focus on packet transport and those that focus on application delivery. Although these can be one in the same, we don't recommend it; separate core competencies are involved. And network architects agree.

Only 24% strongly agreed with the statement that their primary networking vendor can supply the right technology to solve most application performance and security issues.

Conclusion

Today's network architects are in a unique position. Unlike network operations, they are not as bogged down with the day-to-day maintenance of the network. Instead, they have the authority and skill set to explore emerging application issues around security, availability, and performance. How? From a technology perspective, we see the need to adopt products like application-fluent load balancers, application accelerators, WAN optimization, SSL VPNs, and application firewalls — that are all tied together in a single policy-driven application delivery platform. This application delivery infrastructure allows network architects to securely deliver emerging Web applications to any corporate and non-corporate user, improve business continuity, and address bandwidth and latency issues across any network topology. This results in not only reduced operational costs for IT, but more importantly it creates flexible, agile architectures to quickly meet changing application needs.

Appendix

Research Methodology

In March 2007, Forrester Consulting conducted a phone survey of 153 IT decision-makers and influencers across North America, Europe, and Asia-Pacific as part of a study commissioned by Citrix Systems. In this survey:

- Fourteen percent of respondents were senior-most decision-makers in the company, 27% were executives in IT, and 59% were managers or directors of IT that report into an executive in IT.
- Twenty-nine percent of respondents had authority over all of IT, 27% had authority over IT infrastructure and server operations, 22% had authority over desktop or client services operations, and 22% had authority over network architecture.
- One hundred and one respondents were from North America (US and Canada), 27 were from Europe (UK, Germany, and France), and 25 were from Asia-Pacific (China).
- Four percent of respondents were from enterprises that had 500 to 999 employees, 58% had 1,000 to 4,999 employees, 19% had 5,000 to 19,999 employees, and 19% had 20,000 employees or more.
- Thirty-six percent of respondents were from companies with revenues less than \$500 million, 11% were from companies with revenues of \$500 million to \$1 billion, 22% were from companies with revenues of \$1 billion to less than \$10 billion, and 11% were from companies with revenues greater than \$10 billion. Twenty percent of respondents did not disclose company revenues.
- Respondents represented a broad range of industries.