

7 Key Requirements for Secure Remote Access

The world is more dynamic and unpredictable than ever before and market forces are driving change at an unprecedented rate — across both business and technical dimensions. Therefore, rapid access to business applications and information from anywhere has become a critical requirement for modern organizations. The simple fact is that businesses today run on applications, from ERP to email, and from packaged vertical solutions to custom Web applications. Virtually every business project today depends on the ability to get applications to the people who use them in the fastest, most secure, most cost-effective way possible.

Table of Contents

- 2 **Selecting the Right Application Delivery Infrastructure**
- 3 **Requirement #1: Give users easy access to business resources from any location or device**
- 4 **Requirement #2: Find a solution to minimize your cost of ownership**
- 4 **Requirement #3: Find a solution offering comprehensive and extensible endpoint analysis checks**
- 5 **Requirement #4: Find a vendor that can provide an integrated application delivery infrastructure**
- 7 **Requirement #5: Find a solution that supports granular authorization policies and true application-level control**
- 8 **Requirement #6: Find a solution that overcomes the limitations of network access control**
- 8 **Requirement #7: Find a vendor with a staying power, a global reach and a strong vision**

Selecting the Right Application Delivery Infrastructure

Organizations first addressed the need for secure access with IP Security (IPSec) virtual private network (VPN) products to provide network-level access to servers in the data center, but as users demanded access from more locations, the limits of this technology became obvious. The IPSec protocol was often blocked by firewalls and Internet Service Providers (ISPs), and IPSec client software proved difficult to install and manage. This approach failed to deliver on its promises and left users unable to access information in all situations.

To address these shortcomings and improve user productivity, a new class of VPNs was developed utilizing the Secure Sockets Layer (SSL) open standard and more recently, Transport Layer Security (TLS) protocols, to encrypt VPN traffic. This approach allowed remote users to utilize the same protocols used to secure access to websites, providing simpler installation and management and better connectivity, and reducing help desk calls. These products are known as SSL VPNs.

Once VPN technology had evolved to allow ubiquitous access, a new set of challenges emerged. Organizations had no easy way to deliver the wide range of business applications required to utilize information, or to protect sensitive intellectual property from being left behind on shared devices, such as Internet cafes or home machines.

Properly addressing this challenge requires a comprehensive architecture that extends beyond traditional point solutions to control not only what a user can access, but also to enforce policies determining how access occurs. With an integrated application delivery infrastructure, an SSL VPN works in conjunction with client/server, Web and desktop application delivery components in the datacenter to ensure applications and information are available via the most secure and optimal method. Such a solution removes the need to access and store critical information on untrusted clients, eliminating the trade-off between accessibility and security.

Use this guide to get more information about these technologies and learn how they've solved the most critical issues in providing remote access. Then, you'll be equipped to ask vendors the right questions and have the information you need to plan a best-of-breed architecture.

Requirement #1:

Give users easy access to business resources from any location or device.

Your top priority is to provide users with an access solution that is easy-to-use, nearly transparent and responsive. Many products only focus on the mechanics of access and are not designed for usability. Look for a solution that meets these criteria:

- **All client connections should be secured with a protocol accepted anywhere on the Internet.** IPSec provides a strong level of security but is often blocked by firewalls and Internet Service Providers. SSL and TLS protocols are widely used on the Internet to secure website access; support for these protocols is built into all modern Web browsers. Most firewalls and ISPs permit these protocols by default, resulting in fewer rejected connections and less user frustration.
- **Users need access from devices when client software can't be installed.** SSL VPNs introduced a significant improvement by enabling basic access to files, email and Web resources hosted on the organization's network from any client device with a Web browser.
- **Make sure all applications are supported.** Many vendors promise support for all applications but these claims need to be investigated. Do you plan to support VoIP softphones running on roaming laptops? While VoIP solutions claim to use standard protocols, many of them have vendor-specific implementations. Make sure your VPN has been tested with your telephony solution.

You should also investigate applications that require server-initiated connections such as active FTP, some instant messaging solutions and systems management software. Many SSL VPNs don't support these protocols, so make sure your selected solution does.

- **Users shouldn't have to choose the right method of access.** Many SSL VPN products evolved as a combination of disparate technologies and often put the burden of choosing the right access method on the user. This requires users to be aware of a number of technical considerations: Is the VPN client active or am I using browser-only access? Do I need to modify the proxy setting of my applications?

A better way is to allow the remote access solution to detect client capabilities and automatically apply the best means of access. Users shouldn't have to be concerned with how access is provided. Instead, the right method of access should be applied automatically.

- **Users should have a good experience even over a poor Internet connection.** How responsive is your solution when users have a low-bandwidth, high-latency network connection? Do you need to support users in remote, satellite offices? If so, your solution should optimize the traffic to ensure the best experience.

Requirement #2:

Find a solution to minimize your cost of ownership.

Your initial investment is only a fraction of the total cost associated with any remote access solution. You must also consider less-tangible costs of training, support and maintenance. Here are some key factors to keep costs down:

- **A good user experience equals a lower cost of ownership.** A solution that is intuitive and enables easy access from any location will require less training and result in fewer support calls from frustrated users.
- **Administrators shouldn't have to install and maintain software on each client device.** Another key consideration for remote access is the level of touch required for each client machine. SSL VPNs have overcome the end-point maintenance requirements that existed with IPSec VPNs by providing Web-deployed clients. Some solutions will also auto-update these clients when newer versions become available. With these capabilities, administrators are no longer burdened with the task of directly administering each client device.

Requirement #3:

Find a solution offering comprehensive and extensible endpoint analysis checks.

When providing access from a client machine over the Internet, your organization no longer has control over how the clients are configured. To mitigate the risks of malware, make sure the solution you choose meets the following criteria:

- **Client configuration should be checked before allowing access.** Checks can be performed to verify basic security configurations by ensuring up-to-date anti-virus and personal firewall software is active on the client. Clients should also have the latest version of the operating system and browser.

By running an endpoint analysis scan at the beginning of any remote access session, you can detect an improper configuration that may prevent users from authenticating, or limit the permission of the user during the session.

- **Configuration checks should run continuously to detect changes during the session.** Simply checking configuration at the beginning of a session is not sufficient since sessions may last for hours or days. Instead, configuration checks should run on a continuous basis to ensure the user hasn't disabled security software.
- **Choose a solution that provides simple machine identity scans.** In addition to detecting the configuration of a client machine, it's important to determine who performed the configuration. Machines issued and imaged by an organization should be granted a higher level of trust than other devices. In the past, the only way to identify machines was with client certificates — an approach that placed a burden on the IT organization. Instead, choose an SSL VPN that provides alternative identification methods requiring less administrator involvement, such as MAC address verification, domain membership and device watermarking.

Requirement #4:

Find a vendor that can provide an integrated application delivery infrastructure.

Ubiquitous access from any location and any device will be a primary goal for your remote access solution. This means users can gain access not only from their company-issued laptop, but also from any other machine — including ones that may be shared.

Consider the types of resources that you users need access to: files, email, databases, etc. Fortunately, most SSL VPN solutions can satisfy this requirement with IP tunneling or browser-only access.

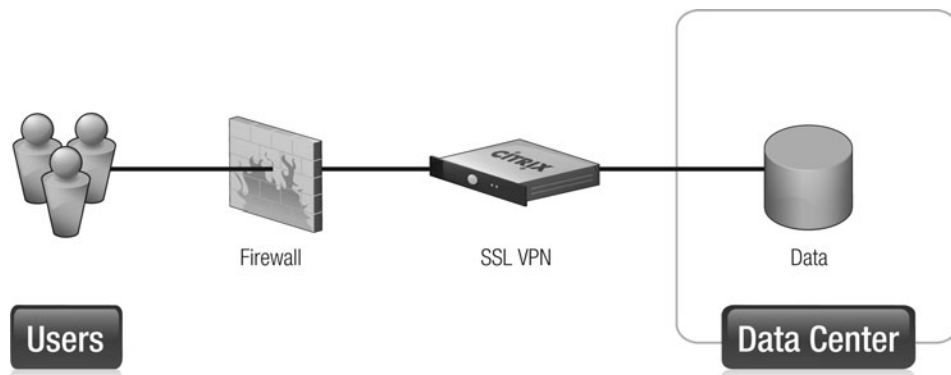


Figure 1 — Traditional Access to Data

Unfortunately, traditional VPN solutions have ignored other key requirements to ensure access remains secure, convenient, and cost-effective. Make sure you choose a solution that ensures:

- **Users always have access to applications.** Documents and information are useless unless users have applications to view the data. While this concept seems basic, most VPN solutions are designed to access data but ignore the need to provide access to the associated applications. Without this capability, they fail to deliver on the promise of true on-demand access, and users will be limited to information accessible from applications pre-loaded on the client machine (assuming the correct application version is available).

For example, SSL VPNs will give users access to their Microsoft® Office documents, but the client device may not have Office installed locally to view these files. With an integrated application delivery solution, a user can use a browser to navigate their files and then view them with an application delivered from the data center — client-side installation isn't required!

Make sure you choose a vendor with integrated product offerings to serve applications to any remote client, regardless of the hardware configuration and base operating system.

- **Intellectual property should be protected.** How can you prevent sensitive data from being inadvertently saved on a home PC or a borrowed machine? Multiple approaches are required to ensure data is only seen by the intended user.

The first line of defense should occur at the Web browser with proper HTTP cache directives preventing data from being cached in the first place. A browser cache cleaner agent will also remove sensitive data at the end of the remote access session. This agent is Web-deployed and wipes the cache, cookies and browser history.

Some SSL VPN solutions provide secure desktop functionality that attempts to isolate and encrypt all data saved to the client during the session, and remove it after the session terminates. This approach requires software installation on the client — not a viable solution for all devices, and requires that sensitive data be downloaded to the client. However, recent announcements of security risks by some vendors demonstrate the limitations of this approach. Often, data will leave the control of the secure desktop environment and be stored in common areas of the client operating system such as virtual memory page files and printer spoolers, making it accessible after the session terminates to anyone with access to the client machine.

A better solution would be to avoid transmitting this data in the first place. A key benefit of integrated application delivery is that data remains in the data center and users interact with it virtually. Best of all, no client components need to be installed, so the solution works from any device.

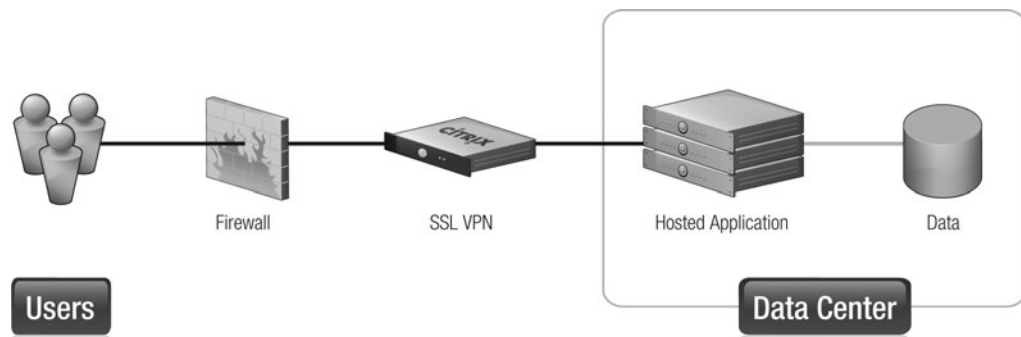


Figure 2 — Virtualized Access to Data

Figure 2 shows an integrated application delivery architecture with an SSL VPN deployed in conjunction with one or more application delivery controllers. As a result:

- Applications are always available to any client machine
- Applications never have to be pre-installed
- Access to applications can be entirely virtualized
- Data never has to leave the data center

Requirement #5:

Find a solution that supports granular authorization policies and true application-level control.

Many remote access solutions force organizations to choose between security and accessibility. The result either favors the user by risking intellectual property with too much access, or favors the information security policy with too many restrictions, forcing users to find creative ways to access the data and applications they need.

By choosing a solution that provides granular, application-level security controls, you can avoid the compromises. Here are the key considerations:

- **Administrators need granular control over the information that can be accessed.** Early VPNs either lacked access controls or only provided control at the network level. The result was that organizations granted users too much access because application-level permissions couldn't be enforced on specific websites and file servers. Some SSL VPNs now allow permissions to be defined down to the resource due to an awareness of application protocols.
- **Level of access should vary based on access scenario.** Would your organization allow users to access sensitive financial records or applications from a home PC or other shared device? Probably not, but that policy is probably different if the user is accessing from a desktop or corporate-issued laptop. By answering some basic questions for each client, your remote access solution can identify the access scenario for each session and adjust rights accordingly. Examples of these questions are:
 - Where is the client located (on the LAN, the Internet or a remote office)?
 - Is the device issued by the organization?
 - Is it a desktop or laptop?
 - Is the device properly configured?
 - Is the device shared by other users?

Only a few SSL VPNs offer organizations the ability to answer these questions and define access policies based both on who the user is AND what the access scenario is, but this capability is necessary to fully protect information.

- **Strict control of action rights should exist.** Scenario-based access control determines which documents or applications can be accessed, but controlling how information is accessed requires application fluency that's only available with an integrated application delivery infrastructure.

Controlling the actions a user can take with resources allows organizations to properly balance security requirements with the access needs of their users. With action rights control, an administrator can define policies that grant full download permissions to a document when the user is accessing it from a desktop within a remote office, or from a trusted corporate laptop. When the user moves to a shared or untrusted device, the policies can automatically adapt to give limited access with a virtual session delivered from the datacenter. Inside this virtual session, policies can control the functionality of the application to ensure files can't be saved to the client device, and that local printers can't be accessed.

Requirement #6:

Find a solution that overcomes the limitations of network access control.

Network access control (NAC) solutions have emerged as a solution to help bolster the security of an organization's network by limiting access when a client does not meet the minimum configuration defined by the security policy. NAC approaches are still emerging and enforcement approaches continue to be problematic or expensive. Some require the replacement of existing network infrastructure such as switches and routers, and others that control the distribution of IP addresses can be easily bypassed by configuring clients with static IP addresses.

An SSL VPN with endpoint analysis capabilities deployed at the edge of the datacenter provides an alternative to NAC. This approach doesn't have to be limited to remote access. Certain vendors provide high-performance SSL VPNs that can scale to support all users in an organization, allowing IT to control access for all devices on the organization's proprietary network.

When planning an NAC solution, a key consideration is the rigorous limitations it places on users by requiring their clients to be configured properly all the time. While this practice ensures strict compliance with security policy, it has associated opportunity costs that are often overlooked. For example, an employee may need to borrow a computer to complete a time-critical task. How much time is required to properly configure this machine? Is it even possible to configure this machine from a remote location? What is the impact to your business if your employee fails to complete this task in time? What if this task was accessing a critical sales presentation to present to a potential customer? Was the protection offered to your infrastructure worth the burden placed on the user? No organization should be faced with this dilemma.

When a user requires access in the example above, the endpoint analysis can determine if the client is properly configured. If so, the information can be downloaded directly to the client to allow the user to complete the task. If the client is configured with the wrong operating system or personal firewall, standard NAC solutions would simply deny access. With an integrated application delivery solution with action rights control, this scenario can be detected and access to the requested data can be provided virtually — allowing the user to complete the task on an untrusted device without the risk of losing valuable intellectual property.

Requirement #7:

Find a vendor with staying power, a global reach and a strong vision.

Any remote access solution you implement will be a strategic and critical part of your network infrastructure. You can best protect your investment by choosing a vendor that can offer a high level of support over the lifetime of your implementation.

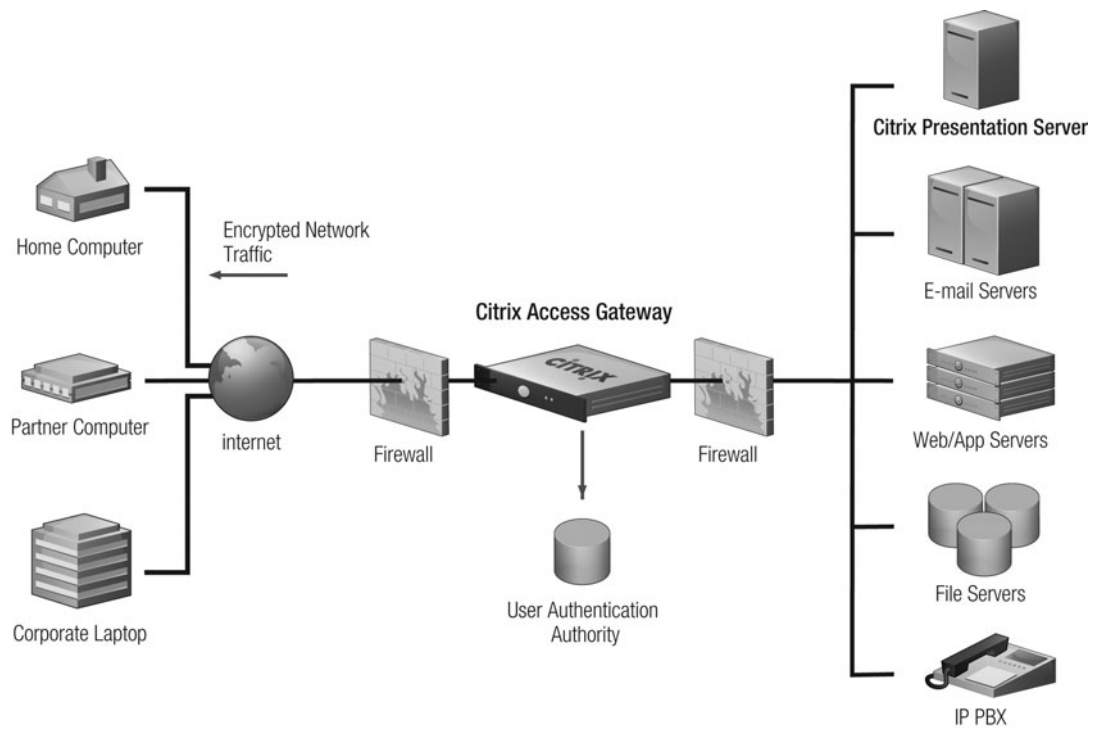
INTRODUCING CITRIX SYSTEMS, INC.

Citrix Systems, Inc., (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 180,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the

Fortune 100 companies and 98% of the Fortune Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. With its revenues of more \$1.1 billion in 2006, you can be assured that Citrix will continue to offer the products and worldwide support that are needed to build your integrated application delivery architecture.

CITRIX ACCESS GATEWAY

Citrix Access Gateway™ is ranked by key industry analysts such as Gartner and Forrester Research as a leading SSL VPN product line. Deployed as a hardened appliance at the perimeter of an organization's network, it gives users a single point of secure access to applications and resources hosted in the datacenter.



PROVIDING A GREAT ACCESS EXPERIENCE

With a Citrix Access Gateway solution users on any client with a Web browser and Internet access can establish a secure connection back to the corporate network and be productive wherever they go.

With an easy-to-use and intuitive interface, users receive the best possible experience, minimizing training and support calls. Features such as always-on access ensure sessions are automatically reconnected after losing a network connection, or when users roam between access points.

Citrix Access Gateway simplifies access from any machine by hiding the complexities from the user. Access can be challenging for a number of reasons. With other SSL VPN products, users often cannot gain full network access because they don't have administrative right on the client machine. The Citrix Access Gateway client installer will detect this situation and automatically install in non-administrator mode, allowing users to use all TCP and UDP protocols without reconfiguring applications.

In situations when client software can't be installed or when users need quick access from a borrowed machine, Citrix Access Gateway enables access to protected websites, file shares and email from any device with a standard Web browser, including some handheld and small form-factor devices.

STRONG SECURITY FOR APPLICATIONS AND DATA

For administrators, Citrix Access Gateway acts as a point of control to secure your organization's vital resources with a number of key capabilities:

- Endpoint analysis can be run on clients prior to authentication and continuously to determine the machine's configuration and identity. Scans are included to detect:
 - Most antivirus software (and ensure an up-to-date pattern file)
 - Personal firewalls
 - Operating system and patch level
 - Browser type and version
 - Known MAC addresses
 - Client certificates
- Clients failing to meet the minimum configuration requirements can be given limited access and sent to remediation pages to install the correct software.
- Users can be authenticated with a number of strong forms of authentication including smartcards and various token-based methods, or from any authority that supports RADIUS or LDAP protocols.
- All communication with the client can be safely transmitted over the Internet because of strong traffic encryption with SSL and TLS.
- Application fluency allows administrators to create granular authorization policies on a number of the most common resource types. By understanding application protocols, Citrix Access Gateway enables administrators to easily control access to Web applications, file shares, email, applications hosted on Citrix Presentation Server™, and any other applications requiring TCP or UDP connections to the data center.

-
- Administrators can grant or deny access to resources based user identity and group membership (derived from LDAP or RADIUS authorities). In addition, policies can be based on the client's access scenario (defined by client configuration, machine identity or network location), allowing access permissions to change as users move between machines.
 - Patent-pending Citrix® SmartAccess technology with Action Rights not only controls what resources a user can access, but also determines the most secure and optimal way to provide access.
 - User and administrator activities can be tracked with the auditing capabilities of Citrix Access Gateway. Optionally, log entries can be sent to an external Syslog server to consolidate entries with other products in the network.
 - With a number of redundancy options, Citrix Access Gateway ensures sessions remain uninterrupted when a single appliance or an entire datacenter site becomes unavailable.

SIMPLE ADMINISTRATION AND LOW TOTAL COST OF OWNERSHIP

Citrix Access Gateway is loaded with features to reduce administrative tasks. With an auto-downloading and auto-updating client, there is no need to touch every client machine. Users can launch any Web browser and deploy the software required to gain access from most Windows® desktops, and Linux, and Mac OS X clients.

Centralized administration allows management of all appliances from a single console, and role-based administration allows organizations to delegate responsibility to multiple individuals.

SNMP support minimizes the need to regularly monitor each appliance for health and performance status, allowing Citrix Access Gateway appliances to notify common network monitoring and management systems when notable events occur.

With capabilities such as multiple authentication points and virtual servers, a single appliance can be configured to support many diverse segments of the user population. Company employees can be directed to a dedicated logon page and authenticate to the standard corporate directory. Partners can use another URL to access a separate logon page and authenticate to a directory containing partner accounts. The same technique can be applied when new companies are acquired, allowing rapid access to information without requiring user accounts to be merged with the main company directory. As new requirements emerge, you'll have the flexibility to rapidly meet these new demands with your existing infrastructure and stretch your capital investment further than you expected.

END-TO-END APPLICATION DELIVERY WITH CITRIX PRESENTATION SERVER

Citrix Access Gateway works with Citrix Presentation Server™ to provide the most fully integrated application delivery infrastructure on the market. The combined solution gives users the best access experience and ensures the tightest control of business-critical resources.

Citrix Presentation Server hosts applications on servers in the datacenter and provides virtualized access to these applications from most client platforms. The application and its documents remain securely in the data center but are made available to clients over a network connection.

Citrix Access Gateway treats these hosted applications like any other protected resource, acting as a single point of control to ensure secure delivery. Administrators can define policies to determine the applications available to a user, and change this access as the access scenario changes. As users move between clients, Access Gateway

and Presentation Server products work in conjunction to automatically reconnect users to the applications they had previously accessed — a technology called Citrix SmoothRoaming™.

SmoothRoaming will respect scenario-based policies. For example, if users who were accessing a sensitive financial application from the office want to move to a home computer, policies can be implemented to disallow SmoothRoaming from reconnecting to the application at home.

Action Rights can also be enforced with Citrix Presentation Server. Administrators can create policies forcing documents to be viewed in a virtualized environment for the highest level of data protection. Key application capabilities, such as printing to the client's local printer or saving to the client's local drive, can also be disabled by a policy. Administrators gain control over the flow of sensitive information by disabling the ability to save data to untrusted client machines.

With the integrated application delivery infrastructure provided by Citrix Access Gateway and Citrix Presentation Server, users will also benefit because the applications they need will be available from anywhere.

DESIGNED TO MEET THE REQUIREMENTS OF ANY ORGANIZATION

With three editions, Citrix Access Gateway is a comprehensive product line giving you the flexibility to choose the capabilities and price point that's right for your organization.

- **Citrix Access Gateway™** Standard Edition is easy to deploy, simple to manage and the most cost-effective solution on the market. With an Access Gateway appliance in your DMZ, you'll have secure access to your protected resources including applications hosted on Citrix Presentation Server.
- **Citrix Access Gateway™** Advanced Edition is a solution geared for small and medium-sized deployments. It extends access to more devices and users by adding features such as browser-only access to resources, support for mobile devices, and a sophisticated policy engine with extensive SmartAccess capabilities and Action Rights control.
- **Citrix Access Gateway™** Enterprise Edition is the best solution for demanding enterprise environments, offering maximum scalability, performance and flexible management options. Built-in high-availability options support business continuity planning with redundant application pairs and seamless multi-site failover options. Integrated application acceleration and optimization capabilities further increase remote access performance to give your users the best access experience.

More Information

You can find more information on the Citrix Access Gateway product line by visiting <http://www.citrix.com/accessgateway>.

Citrix Worldwide

WORLDWIDE HEADQUARTERS

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

EUROPEAN HEADQUARTERS

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

ASIA PACIFIC HEADQUARTERS

Citrix Systems Hong Kong Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000

CITRIX ONLINE DIVISION

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400

www.citrix.com

NOTICE

The information in this publication is subject to change without notice. THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. THE USE CASES IN THIS PAPER ARE PROVIDED ONLY AS POTENTIAL EXAMPLES AND YOUR ACTUAL COSTS AND RESULTS MAY VARY.



About Citrix: Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 180,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the *Fortune* 100 companies and 98% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Annual revenue in 2006 was \$1.1 billion. Learn more at www.citrix.com.

©2007 Citrix Systems, Inc. All rights reserved. Citrix®, Citrix Presentation Server™, Citrix Access Gateway™ and SmoothRoaming™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and other countries. Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.