CITRIX®

Securely Delivering Applications Over the Internet

White Paper

Table of Contents

Information security in the age of the remote community

Faced with a steady increase in the number and types of remote users they must reach, organizations are constantly looking for faster, more reliable ways to communicate. From mobile workers, telecommuters and international branches to partners, suppliers and customers, these remote users require access to company applications and data at any time and from any location. Trends such as the advent of online commerce, the growth of business-to-business outsourcing for greater efficiency, and the proliferation of mergers and acquisitions have intensified the competitive need to deliver information more broadly than ever.

Application server computing has become a mainstream solution to this challenge. This server-based architecture, which supports multiple server platforms and client operating systems, allows organizations to deploy a variety of applications to remote users on different devices, over different network connections. Further, application serving is enabling the new application service provider (ASP) industry, which offers external application hosting and delivery to customers for a set fee.

Many enterprises and ASPs that have adopted application server computing are turning to the Internet as their preferred network for application deployment, due to its lower cost, greater geographic reach and faster implementation speed. Compared with traditional methods such as modem banks, dial-up to remote access servers (RAS), dedicated leased lines, and electronic data interchange (EDI) services, the Internet can save significant amounts of money, provide true global connectivity, support e-business applications and simplify client device requirements through the use of a browser.

However, because the Internet is a public network, one of the main concerns about using it for application delivery is the security of sensitive corporate information. Although the application server computing model keeps application execution 100 percent on the server, and sends only user interface updates, keystrokes and mouse clicks over the network, most organizations demand additional security features such as encryption and authentication when using the Internet.

Enterprise security concerns about the Internet

Following are the most pressing security issues facing organizations that wish to deliver applications and data over the Internet.

Protecting data.
Because the Internet is public, data traveling across it is at risk for interception or compromise by unauthorized users. Data encryption is often used to thwart hackers; however, there are various types and levels of encryption and each organization must determine what is appropriate.

Restricting user access.
In addition to preventing data access by outsiders, organizations typically need to control which of their users can access which data sources. To achieve this, authentication of both user and server/s can be required.

Traversing firewalls.
The popularity of Internet use has spawned corporate firewalls to protect private, internal networks from untrusted users. For users to reach applications behind firewalls, there must be a mechanism in place to navigate these security barriers.

Integrating existing systems and infrastructure.
The Internet, when used for application delivery, can affect the existing security infrastructure and should be carefully evaluated.

Controlling cost.
Organizations considering the Internet as a delivery network will most likely wish to implement additional security measures that can add costs.

Controlling complexity.
The security measures typically implemented with an Internet-based application delivery approach can make the computing system more complex to administer and use.

Virtual Private Networks for Application Serving over the Internet

Virtual Private Networks (VPNs) are growing in popularity as one of the most effective ways to provide secure remote access to applications over the Internet. Infonetics Research predicts that sales of managed VPNs will surge from $2 billion in 2000 to approximately $25.5 billion in 2004, as they take share from traditional leased-line WANs.

VPNs are private networks built on public or shared network infrastructure, most commonly the Internet. A VPN establishes a secure data path, or "tunnel," using encapsulation protocols defined by standards such as IPSec or PPTP to transfer information over the network. VPNs offer organizations a number of advantages over current access methods: modem banks can create an administrative nightmare as organizations are forced to upgrade and expand access capacity to support additional users; dedicated leased lines, the most common alternative to modems, are usually very expensive and are not available outside the office.

VPNs can significantly reduce the telecommunications costs associated with remote application delivery by replacing expensive dedicated lines, modem banks and dial-up toll charges with a local call to the user's Internet Service Provider, DSL or cable access company. With VPNs, users securely access the largest possible bandwidth to receive ubiquitous application access from Web browsers. Because they are billed on a usage basis, VPNs deliver greater ROI than dedicated leased lines or modem banks that create overhead but may be used only a portion of the time.

For many companies, the attraction of VPNs is expanding beyond cost; a key benefit in today's Internet economy is their ability to securely connect outside users, such as suppliers, consumers or business partners, to corporate applications. For ASPs, whose core business is connecting outside clients with applications hosted in data centers, a high level of security is an essential component of their value proposition.

VPNs are viewed as an enabling technology for e-commerce applications. They are also seen as a way to reduce the costs of providing information to remote users, especially those in international locations. Other benefits include rapid implementation, especially when compared to dedicated lines; the broadest geographical reach of any access model; and the ease of use and wide availability of Web browsers.

VPNs offer important advantages over other commonly used Internet-based access solutions. E-mail, which is a store and forward system, cannot deliver applications or real-time access to information. It also requires large amounts of data to be sent or copied to multiple locations. Secure Socket Layer (SSL) traditionally allows secure data exchange with Web pages. This support has been expanded in some products to include applications and additional client-side authentication, where previously only server authentication was provided.

Two commonly used Internet VPN architectures are network tunneling and client-to-enterprise. Both employ encrypted tunnels; however, in network tunneling, the user receives access to all resources, including all servers, workstations, applications, email, databases, etc. A client-to-enterprise VPN can control the user's access, ensuring each individual receives only the resources he or she is permitted.

This access control at the "end of the tunnel" gives organizations an additional security tool.

Access control is complemented by authentication, the process of requiring users to prove their identity before establishing a network session, and ensuring the user is connecting to an authorized application server. According to an article in the May 8, 2000 issue of InternetWeek, "Increasingly, IT managers are looking for more robust ways to ensure the user is who he or she claims to be. User name and password approaches are fine in many cases when you are letting your own employees access their e-mail at night via direct dial-in. But companies need something stronger when doing business over the Internet."

Both access control and authentication must be supported by encryption, which is data "scrambling" or ciphering to make sure the transmitted content cannot be read by unauthorized users. For the optimal level of security, a VPN solution needs to provide all three elements. In addition, to reach users efficiently a VPN must be able to traverse defensive firewalls using ports that administrators already have open and will accept Web-delivered information.

Comparing VPN Solutions

The VPN market is still growing, with a variety of solutions to choose from. Because of the strong concern about security over the Internet, these options are often evaluated on the basis of their security offerings, as well as cost, complexity and scalability. Although many people think of hardware solutions such as appliances and routers, VPN software offers greater flexiblity as well as other benefits.

With software, access control is not wide open as a policy but rather is closed, with access granted only to specific resources. Software supports a variety of authentication methods — not just hard devices such as IPSec, but also tokens, Smart Cards and Public Key Infrastructure (PKI). These solutions are easier to use across organizations because they are not dependent on hardware and firmware compatibility.

Within the software VPN category, there are further distinctions. Most solutions are Windows-centric and do not support other server or client platforms, limiting the flexibility of application deployment. However, Citrix® Extranet™, a new VPN software solution from Citrix Systems, Inc., meets the need for comprehensive security as well as support for diverse server and client platforms, including thin devices.

Citrix Extranet

Citrix Extranet provides a virtual private network (VPN) which allows you to securely deploy the latest business-critical applications to users around the world, via the Internet — all while maintaining the manageability, scalability, reliability and control you've grown to expect from Citrix. Supporting site-to-site configuration, it provides an exceptionally high level of security for enterprises and ASPs using a server-based computing model. It delivers secure communications over the Internet between the Citrix Extranet client and the Citrix Extranet server. The solution, which can be installed on its own server or on a firewall, supports a wide range of client operating systems, including Microsoft® Windows NT®, Windows CE/PocketPC, Windows 95, Windows 98, Windows 2000, Macintosh, Linux® and Sun Solaris™, and server platforms, including Windows NT and Sun Solaris.

Citrix Extranet supplies all three types of safeguards — authentication, access control and encryption — required for the highest level of VPN security:

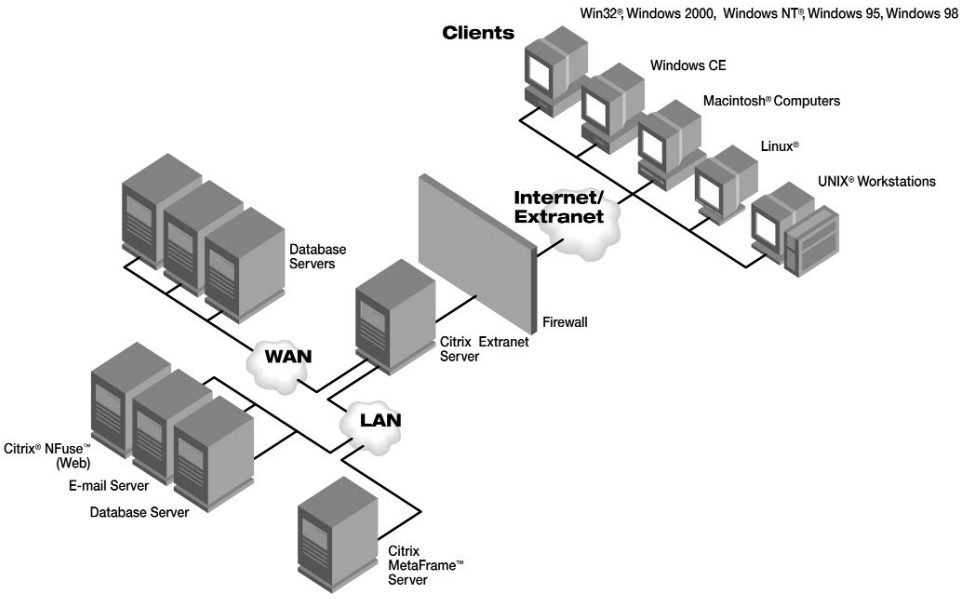
- **Authentication.** Considering the millions of individuals and organizations with Internet access that could potentially intercept a VPN transmission, a key component of VPN security is obtaining proof of a user's identity before establishing a connection for that person to applications and data. Citrix Extranet uses a two-factor authentication system comprised of a digital token, digital certificate or "smart card" that the user has, and an access code that the user knows.
- **Access Control.** Authentication goes hand-in-hand with controlling access to resources. Typically, organizations do not want every user or group to have access to all the applications and data on the system. To limit authorized users to the information they are allowed, Citrix Extranet assigns access permissions on a per-user, per-group and "all" basis. Once a user is authenticated, the system contacts every server for which that user has an authentication key and requests current permissions. The user is given access only to those servers and URLs for which he/she has current privileges.
- **Encryption.** Although it is the basic method for keeping information private on the Internet, encryption can negatively affect connection performance. Further, scaling up the distribution of encryption keys can be problematic. Citrix Extranet solves these challenges by applying two different encryption technologies at different stages of deployment: public key encryption during the online registration process to enable remote users to receive and register their encryption keys; and the use of Triple Data Encryption Standard (3DES) to create an identical key on the server. Shared key encryption is computationally simpler than public key technology, offering performance advantages necessary to support business applications over VPN connections.

In addition, Citrix Extranet allows firewall traversal without requiring intervention by the firewall administrator. This capability is especially important in ASP scenarios and extranets where the VPN encounters many different firewalls protecting customer, partner and supplier organizations. Citrix Extranet configures clients to use Internet port #443 or #80, which are already open to Web traffic, rather than opening a non-standard port.

Citrix Extranet Benefits

Citrix Extranet addresses the challenges of deploying applications quickly and securely to large extranet user populations, while providing the manageability, scalability, cost benefits and ease of use that characterize Citrix application server solutions.

- **Flexible Integration.** Citrix Extranet integrates with existing Citrix application server environments and existing security infrastructures. It allows the use of third-party authentication systems, such as "smart cards," tokens, PKI, and RADIUS, and works with virtually all firewalls.
- **Rapid Deployment.** Citrix Extranet uses On-Line Registration (OLR) to quickly and efficiently distribute VPN access credentials to remote users. OLR allows shared secret keys and user IDs to be generated without interaction from an administrator, and enables users to begin accessing the system within a few minutes. Looking at the larger picture, Citrix Extranet allows users to connect to applications faster because no special hardware needs to be implemented.
- **Centralized Management.** Citrix Extranet Admin gives administrators the ability to configure multiple Citrix Extranet servers remotely, using the Citrix Extranet client, or locally on a Windows NT platform. To efficiently manage user access, the solution allows administrators to download valid access permissions through Dynamic Configuration. Groups, or individuals can be given access to TCP/IP services or Web URLs.
- **Simplicity and Ease of Use.** Citrix Extranet simplifies the establishment of VPN connections by remote users through a simple, two-step client activation process. Users install the client software using the friendly Windows Wizard program and then register online.
- **Cost-Effectiveness.** By supporting multiple server and client platforms, Citrix Extranet allows organizations to leverage their existing computing systems. It also saves the cost of installing and managing expensive, complex leased lines or modem banks. Further, centralized client management and electronic user registration reduce support costs.



Conclusion

Virtual Private Networks offer the best solution for delivering applications securely over the Internet, thanks to their added security, rapid implementation, cost savings and global reach. Choosing a VPN platform should include evaluation of specific security features, cost and complexity, manageability, client and server support, and ease of use. By selecting Citrix Extranet, a VPN software solution that offers powerful, end-to-end security combined with centralized server and client management, organizations can have confidence in their ability to quickly and securely deliver application access to their extended workforce, business partners, suppliers, and customers over the Internet.

Glossary of Terms

3DES. Cipher that applies the DES cipher three times with either two or three different DES keys. The Citrix Extranet implementation uses three DES keys (2168 combinations).

Access Code. The secret code — similar to a PIN on an ATM card—required to unlock the authentication key stored on the user's token each time the user accesses a secure service. This code, defined by the user during registration, must be at least four characters in length with a maximum of 16, and can be any combination of letters and numbers.

Access Control. Allowing or denying connections through the use of access permissions.

Access Permissions. The associations between users and connections, as defined by a User ID, group name, service (TCP or Web), or destination. Citrix Extranet access permissions can be either individual user permissions or group permissions.

Authentication. The process of determining the identity of a user attempting to access a system.

Authentication Key. The key is a 32-character hexadecimal key assigned to a user during installation by the registration server administrator, consisting of the numbers 0 to 9 and letters A to F.

- The Citrix Extranet authentication system supports virtual smart cards and ISO-standard smart cards for both authentication and stored data. A user with a physical smart card must use a smart card reader connected to their PC. Virtual smart card information (FIPS or VCAT token) may be stored on either the PC hard drive or a removable (floppy) disk.
- The user's Citrix Extranet authentication key is stored on the smart card, whether physical or virtual. This information is shared with the Citrix Extranet Server, where it is stored in the Citrix Extranet Server's user database.

Authentication Token. A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques.

Authenticator. The name assigned to a Citrix Extranet Server through which users can access a particular service. This name can be up to 14 alphanumeric characters in length and it is recommended that it be a derivative of your Citrix Extranet Server hostname.

Domain Name. Identifies a 'location' on the Internet (e.g., citrix.com) that has been registered with the Internet Network Information Center (InterNIC). Currently the domain name is limited to 47 characters. Through the use of aliases, however, it is possible to accommodate longer names.

DES. Data Encryption Standard is a NIST-standard encryption algorithm for secure data protection. A binary number is used as an encryption key with 720 quadrillion possible combinations (256). The key is randomly generated for each session (TCP connection).

FIPS Token. (Virtual Smart Card or Soft Token) A software emulation of a hardware authentication token that is in compliance with the FIPS140–1 coding standards. It stores your private information (authentication key) in an single encrypted file, either on a floppy disk or on your hard drive. FIPS Token is the default authentication method.

OLR. Citrix Extranet provides On-Line Registration (OLR) services which you may wish to implement depending on your system configuration and the functional requirements of your organization.

RC4. Developed by RSA Data Security, Inc., this variable key-size stream cipher uses byte-oriented operations to perform random permutations. The typical cipher period is greater than 10100. Since eight to 16 machine operations are required per output byte, the cipher runs very quickly in software. It is commonly used for secure communications, such as encrypting secure Web site traffic using the SSL protocol.

VCAT Token. Identical to the FIPS Token, except that it stores your private information (authentication key) in an encrypted file system, rather than a single file.

Virtual Private Network (VPN). A private network created over a public network (e.g., the Internet) by using encryption, where exclusive client and host communications can occur.

Worldwide Headquarters
Citrix Systems, Inc.
6400 NW 6th Way
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000
http://www.citrix.com

Americas Headquarters
Citrix Systems, Inc.
6400 NW 6th Way
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 437 7503

European Headquarters
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

Asia Pacific Headquarters
Citrix Systems Asia Pacific Pty Ltd.
Level 3, 1 Julius Avenue
Riverside Corporate Park
North Ryde NSW 2113
Sydney, Australia
Tel: +61 (0)2 8870 0800

CITRIX®

Now everything computes.™

BALTIMORE™
www.baltimore.com

6073E/R1/0800/500