

Strong Authentication For Secure VPNs

Executive Summary

Virtual Private Networks (VPNs) are the de facto standard for providing remote access to mobile employees, partners, customers and suppliers. For most applications, VPNs based on Secure Sockets Layer (SSL) protocol are an optimal solution because they do not require third-party client software and are easier to support and maintain. Citrix Access Gateway™, a family of SSL VPNs, offers several advantages for remote access systems, including its comprehensive functionality, ease of implementation and operation, and the ability to fully control remote access to applications and data for individual end users.

VPNs protect data and applications transmitted over network by creating a secure tunnel between the host and remote access point. However, they do not control access to either end of the tunnel itself. Because the integrity of a VPN solution, and the enterprise network itself, depend on access only by authorized users, a strong user authentication system will add an incremental level of security to protect the VPN from intrusion. Gemalto's Strong Authentication solution delivers an unsurpassed level of identity protection with a family of portable and convenient end-user devices. It also enables organizations to implement mutual authentication and more comprehensive identity protection and network security solutions without being forced to abandon infrastructure investments or change end-user devices.

Citrix and Gemalto have worked together to tightly couple their respective VPN and strong authentication technologies. As a result, a secure remote access solution for multiple categories of users can be deployed using an integrated system that is highly secure, easy to install and convenient for enterprises of all sizes. In particular, financial services organizations, health care providers and government agencies will benefit from the confluence of these two complementary technologies from Citrix and Gemalto.

Table of contents

Executive summary2

Introduction.....4

Citrix Access Gateway5

Strong Authentication Makes VPNs Secure5

Gemalto’s Comprehensive Strong Authentication Platform6

Conclusion10

About Citrix and Gemalto10

Introduction

This document provides a review of VPN and strong authentication technologies and presents an overview of Citrix Access Gateway, a VPN solution, and Strong Authentication Server from Gemalto. Its purpose is to demonstrate how these products can be integrated to produce an incremental level of security for remote access systems in order to protect network users as well as their connections to the host network.

On Demand Access From Anywhere

The Internet and private networks are mission-critical assets for organizations of all sizes due to their impact on employee productivity, profitability and competitiveness. Employees, partners, suppliers and customers require on-demand access to data and applications from anywhere using any type of system, including thin clients, wireless devices and laptops. While providing remote access to mobile users is a business necessity, it also makes the network more vulnerable to intruders. Unauthorized network access through phishing, buffer overload and brute force attacks is becoming more common and, at the same time, more difficult to prevent.

Because of the business risk associated with lost data and unauthorized access, enabling and maintaining remote network access systems have become important priorities for IT organizations. When deployed with a firewall, VPN solutions are a proven method of establishing a secure connection between private networks and remote users using cryptographic tunneling protocols. VPNs are widely deployed by organizations throughout the world to securely connect millions of remote users. They offer several advantages, including broad connectivity options, favorable economies of scale, and lower implementation costs. Several alternative VPN technologies are in use today with the two most common being Internet Protocol Security (IPSec) and Secure Sockets Layer.

IPSec versus SSL VPNs

Internet Protocol Security is a mature and proven technology for VPN-based remote access systems. IPSec VPNs were originally designed for site-to-site connectivity and operate at the network layer (Layer 3) of the Open Systems Interconnection (OSI) model. They extend the private network out to a remote computer by providing a secure tunnel between the host computer and the remote client. The security of the tunnel is maintained by encrypting information into Internet Protocol (IP) packets and then decrypting these packets on the receiving end; all packets are protected regardless of content. Users have all of the functionality of the host network with minimal granularity in access control for applications and data.

IPSec VPNs require dedicated hardware at the host location and a dedicated software component that must be installed on each physical device used for remote access. Although more recent operating systems such as Windows XP and Mac OS X include a scaled-down VPN client with limited functionality, most IPSec VPNs use third party client software which must be installed and maintained on each system. This can substantially increase the workload for IT organizations, create service disruptions and add unnecessary operational expenses.

Furthermore, since remote access is only supported on client devices with the correct software installed, connecting from kiosks, public machines and infrequently used devices is difficult. Another limitation of IPSec VPNs is the potential for blockage by firewalls because IPSec exists as a separate protocol within the TCP/IP

stack. In addition, once access has been authorized, most IPSec VPNs have no way of controlling and managing access rights to specific servers, databases or applications.

To address some of these limitations, alternative VPN solutions use standard SSL protocol to create an encrypted tunnel between the server and client. SSL VPNs tunnel traffic at Level 5 of the OSI model, the session layer, as opposed to the network layer. This protocol was originally developed to secure Internet-based commerce and IP applications so by default, all browsers support it and no additional software is necessary. In reality, SSL VPNs function more like a secure application gateway with support for multiple protocols such as http(s) for web applications and Windows Remote Desktop Protocol (RDP) for business and productivity applications.

SSL VPNs do not require dedicated client software and support remote network access from any device that runs a browser. This capability offers a substantial benefit for organizations that need to provide flexible remote access solutions. When compared to IPSec VPNs, SSL-based solutions are less expensive to manage, eliminate security risks of open-by-default tunnels, and offer a superior user experience for employees and business partners who need controlled access to a wide range of applications and resources from remote locations. In addition, deployment and support costs are lower because third party software clients aren't needed, users require less support, and troubleshooting tends to be easier.

Citrix Access Gateway

Citrix Access Gateway products are a family of hardened SSL VPN appliances that can be easily adapted to existing networks and provide users with controlled access to all of the applications and resources they need to be productive. They are optimized for compatibility with the entire suite of Citrix Access solutions, including Citrix XenApp™. Access Gateway products deliver universal secure access to any application or network protocol, including distributed Windows® and UNIX® applications, Web applications, network file shares, and even telephony services using VoIP soft phones — without any custom development or “webification.” Access policies, based on administrator-defined rules and end-point analysis, determine the level of user access. The user experience is comparable to LAN-based access and users are automatically reconnected to their applications and documents when changing locations.

Access Gateway helps organizations overcome the problems associated with other VPN solutions, such as firewall and proxy traversal issues, complex client software distribution, limited application support and management complexity. It provides end-users with a consistent, seamless access experience comparable to working from the office. Access Gateway also eliminates the cost and complexity of installing, configuring, updating and supporting complex VPN solutions and third-party client software.

Strong Authentication Makes VPNs Secure

Although VPNs enable a high level of security for the end-to-end network connection security, they provide limited client-side security. Also, since most organizations use single-factor authentication (i.e., a user name and password) to verify user identities, their remote access systems are vulnerable because user identity credentials can be easily hacked or stolen. If a single user's login

information is compromised and used for unauthorized access through the VPN, the entire enterprise network and network-based assets are at risk.

Single factor authentication makes VPNs vulnerable to attack and increases the risk of online identity theft. These security risks can create substantial operational disruptions and legal liabilities. In addition to stolen digital assets and lost productivity, a network security breach can result in identity theft claims from users whose personal information was stolen, denial of service claims from customers who can't access the company's systems, as well as claims from a third party who may have received malicious code.

To protect against these risks, VPN security can be enhanced by incorporating a strong two-factor authentication system. Two-factor authentication solutions validate network identities by incorporating something the user knows (for example, a user name and password or personal identification number) and something the user has in their possession (such as a security token, one-time password or a smart card). Financial institutions, health care providers and government agencies are increasingly using strong authentication systems to protect their network users and remote access systems.

This type of integrated solution is ideal for mobile users who access corporate applications and sensitive data, including personal, financial and medical information. It also helps ensure compliance with state and federal laws that mandate or recommend the use of strong authentication, including the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Federal Financial Institutions Examination Council (FFIEC) and Family Educational Rights and Privacy Act (FERPA). Several advancements in both VPN and strong authentication technologies, and the level of integration between them, make this type of remote access solution easy to implement and maintain for organizations of all sizes.

Gemalto's Comprehensive Strong Authentication Solution

Gemalto designed a strong authentication solution to incorporate the strengths of its smart card technology. It consists of a family of smart-card based user authentication devices, a browser plug-in, an authentication and customer care server and a self-service user care portal. The Gemalto Strong Authentication Server (SAS) runs under Windows, Linux and Unix operating systems.

With SAS, a user logs on with a user name, password, and one-time password generated by the strong authentication device using an encrypted algorithm. The one-time password is entered using a modified version of the login interface. The request is sent to the Strong Authentication Server for validation and network access. Once the user credentials are checked against information generated by the Strong Authentication Server using the same algorithm, the system either allows or denies network access.

Support for open standards and industry- standard protocols enables hardware optimization, and also helps reduce the total cost of ownership. Gemalto Strong Authentication Server (SAS) has a lower total cost of ownership relative to alternative solutions and provides true anti-phishing security and a variety of form factors for end-users. Organizations can deploy Gemalto SAS for secure user authentication and implement more comprehensive identity protection and network security solutions without being forced to abandon infrastructure investments or change end-user devices. The Gemalto SAS platform can be used for one-time password applications and it supports mutual authentication, PKI, and the smart card-based security features in Microsoft's Windows and .NET platforms. In these implementations, Gemalto SAS can be used to authenticate users to the network while PKI provides encryption, digital signature and transaction security capabilities. The same end-user devices and smart cards can be deployed to support this type of implementation.

An Integrated Solution from Citrix and Gemalto

Citrix and Gemalto have worked together to integrate their respective VPN and strong authentication products so that customers can implement a remote access solution that extends security to end users and protects their identity credentials. Access Gateway offers personalized access to enterprise applications and data from any network access point using any device. With the incremental protection provided by Gemalto SAS, only authorized users are allowed to access these resources through the VPN. This integrated solution helps ensure the integrity of the remote access system and protects against hacking, online identity theft and other forms of attack.

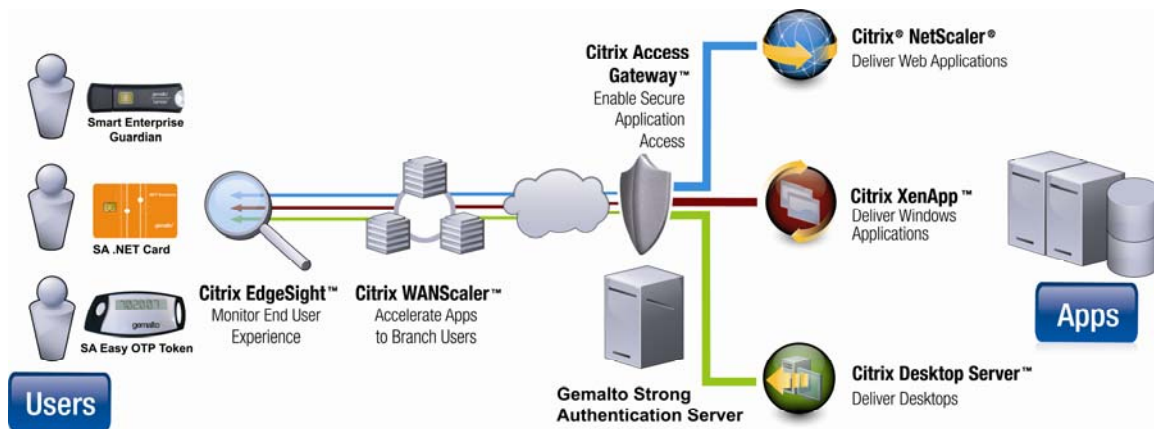


Figure 1. Citrix Access Platform with Gemalto Strong Authentication

Because the two Citrix VPN and Gemalto strong authentication solutions are tightly coupled, IT administrators benefit from an out-of-the box solution that can be efficiently installed, integrated and maintained. Both products are easily integrated with existing network architectures and data servers. For end users, the solution provides all the advantages of VPN remote access and an unsurpassed level of online identity protection using a single customized interface for login.

VPN – Strong Authentication System Deployment

Access Gateway is quick and easy to deploy and simple to administer. The most typical deployment configuration is to locate the Access Gateway behind a firewall or in the demilitarized zone (DMZ). However, more complex deployments, such as those with a server load balancer, are also supported. The Administration Tool is used to configure the basic settings that are specific to the enterprise network, such as the Access Gateway IP address, subnet mask, default gateway IP address, and DNS address. After the basic connection is established, Access Gateway settings are configured for operations such as the options for authentication, authorization, and group-based access control; kiosk mode; end point resources and policies; portal pages; and IP pools.

Once Access Gateway is installed, integrating Gemalto Strong Authentication is a straightforward process. The first steps are to install the Strong Authentication server, load the IAS agent plug-in on to a Microsoft RADIUS server, and record the address and port of the IAS server. The RADIUS authentication option is then selected from the Authentication tab of the Citrix Access Gateway Administration Tool as shown in Figure 1. Next, the secret from the IAS server is entered. Strong authentication is now enabled and custom login screens can be created prior to activating end users.

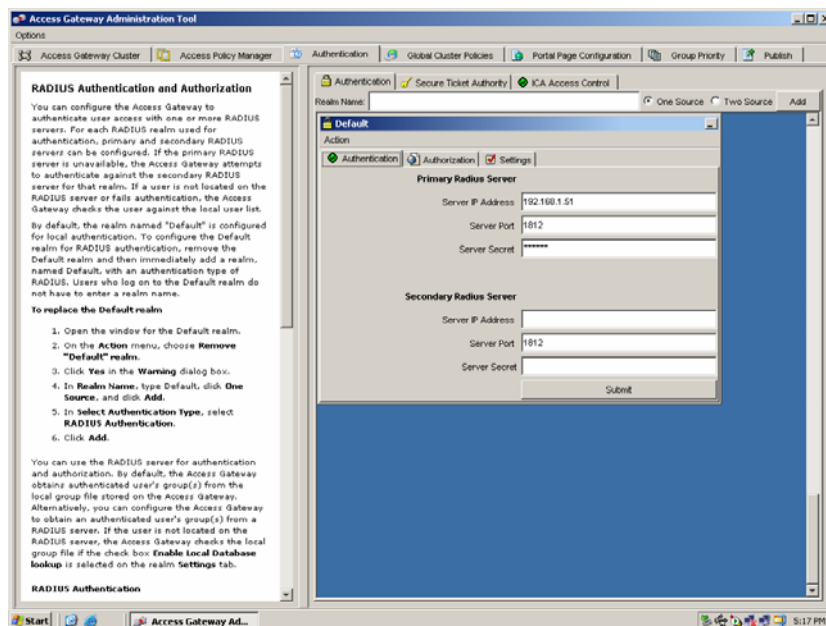


Figure 2. Access Gateway RADIUS Authentication Configuration

User Provisioning and Activation

Access Gateway enables administrators to create customizable multi-factor authentication prompts for user login. This feature is used to configure the appliance so that users can enter the one-time password for network access (Figure 3). Administrators also can create authentication realms for different user categories and specify custom password labels.

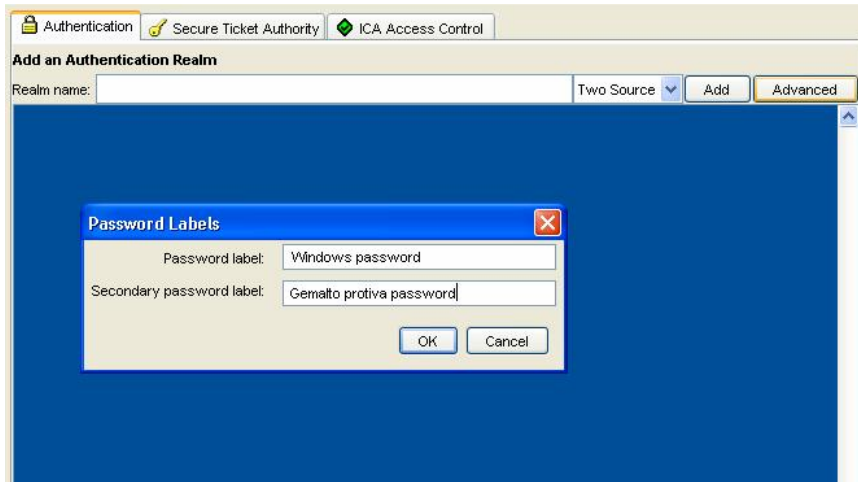


Figure 3. Access Gateway – SAS Secure Login Screen

The SAS Customer Care Portal offers three options to provision and manage end-user smart card devices and authentication credentials: a Batch Client provisioning tool, a Customer Care Interface, and Live Provisioning. The Batch Client provisioning tool enables administrators to create multiple device records at one time and activate multiple users. It is especially useful when setting up a new system since a large number of device records can be enabled in one step.

The Web-based Customer Care Interface supports the administrative functions for managing users and their access privileges, smart card devices and system transactions. It provides the functionality to create or update a record for a Strong Authentication device, link it to a user and activate the device.

The Customer Care Portal also supports Live Provisioning, a fast and convenient way to personalize a new Strong Authentication device or re-use an existing device for end users. Using a Strong Authentication Easy token and a Gemalto contact-less smart card reader, administrators can place the card within the scan area of the reader and automatically create a device record, save it on the data server, and securely transfer the information to the smart card device.

Once the VPN is installed – the Strong Authentication solution operates seamlessly and transparently to the end user. A remote user downloads the Secure Access Client from the VPN by simply connecting to a secure URL, typically the fully qualified domain name (FQDN) of the Access Gateway. When connected, the user enters personal authentication credentials, i.e., user name, password, and a one-time password generated by the Strong Authentication device. After the user successfully authenticates with the Strong Authentication server, Access Gateway establishes a secure tunnel for the remote connection. As the remote user attempts to access network resources across the VPN tunnel, the Secure Access Client encrypts all network traffic destined for the organization's intranet and forwards the packets to Access Gateway. Access Gateway terminates the SSL tunnel, accepts

any incoming traffic destined for the private network, and forwards the traffic to the private network. It also sends traffic back to the remote computer over a secure tunnel.

Conclusion

Virtual Private Networks are susceptible to unauthorized use and hacking but they can be protected by incorporating a strong user authentication system for login and network access. This solution provides a secure tunnel for communications between the user and host network and helps assure that only authorized users access the host network through the VPN. VPNs with strong authentication solutions are being adopted by financial services firms, health care providers and government agencies and are also beneficial for organizations that need to comply with laws that mandate or suggest the use of strong authentication, including HIPAA, Sarbanes-Oxley and FERPA.

About Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 200,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security, and lowest cost. Citrix prosumers include 100 percent of the Fortune 100 companies and 98 percent 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. For more information, visit <http://www.citrix.com>.

About Gemalto

Gemalto (Euronext NL 0000400653 GTO) is the leader in digital security with pro forma 2007 annual revenues of over €1.6 billion, more than 85 offices in 40 countries and about 10,000 employees including 1,300 R&D engineers. In a world where the digital revolution is increasingly transforming our lives, Gemalto's solutions are designed to make personal digital interactions more convenient, secure and enjoyable. Gemalto provides end-to-end digital security solutions, from the development of software applications through design and production of secure personal devices such as smart cards, SIMs, e-passports and tokens to the deployment of managed services for its customers. More than a billion people worldwide use the company's products and services for telecommunications, financial services, e-government, identity management, multimedia content, digital rights management, IT security, mass transit and many other applications. As the use of Gemalto's software and secure devices increases with the number of people interacting in the digital and wireless world, the company is poised to thrive over the coming years. For more information, please visit www.gemalto.com.