



The Security Division of EMC

RSA Solution Brief

Securing SSL VPNs with RSA SecurID® Two-factor Authentication



The need to ensure that only authorized users are granted access is mission critical.

Businesses increasingly need to provide employees, partners and even customers with easy and cost-effective mobile and remote access to corporate applications and resources. The need to ensure that only authorized users are granted access is mission critical. To provide true network security, the access method itself must be bulletproof, and controls must be put in place to manage the identity of the individual who is accessing network resources.

The combination of secure socket layer (SSL) security with strong, two-factor authentication solutions allows organizations of all sizes to cost-effectively safeguard the corporate network while enabling easy remote access to authorized users. RSA, The Security Division of EMC, provides a compelling, two-factor authentication security solution that allows organizations to protect SSL-based virtual private networks (VPNs). The RSA SecurID® two-factor authentication solution, a core component of RSA's Identity Assurance portfolio, is flexible, scalable and simple to administer so that businesses can efficiently provide mobile and remote SSL VPN access to the enterprise while protecting information and applications.

Addressing Remote Access Trends

As organizations become more global in nature, the environment of today's worker is evolving, from one of centralization and control to one of mobility and performance. With an increasing number of mobile and remote workers, a challenge for many of today's organizations is how to provide effective technology tools to maximize the productivity of remote and mobile workers while maintaining a high level of security for critical company information. Opening up access to the enterprise can bring risk to those organizations that do not implement precautions to safeguard valuable information.

Most organizations have limited IT resources to manage a growing base of mobile workers, and often times VPNs become too complex to properly ensure that sensitive corporate information is adequately protected. Therefore, innovative technology solutions are required that can be easily integrated into existing infrastructure and provide end-user "self-service" remediation. This, in turn, simplifies the overall end-user experience and minimizes the need for ongoing technical support. Organizations need the ability to implement secure solutions that address leading remote access trends, including the following:

Identity Assurance

Identity Assurance is the set of capabilities and methodology that minimizes the business risk associated with identity impersonation and inappropriate account use. Identity Assurance brings confidence to organizations by allowing trusted identities to freely and securely interact with systems and access information, opening the door for new ways to generate revenue, satisfy customers and control costs.

The Growing Mobility of the Workforce

The number of remote and mobile workers continues to rise, and an increasing number of employees work from home occasionally. Companies face an increasing need to provide anywhere, anytime access to sensitive information for employees, customers and partners-while at the same time assuring the identity of users and protecting information resources.

Rising Use of Unmanaged Devices for Remote Access

Workers need to access enterprise information from diverse locations, often through unmanaged devices over which the enterprise has little control. There is an increasing use of mobile devices such as smart phones and PDAs for remote access, and end-users are accessing the network from hotel or airport kiosks. Organizations are under increased pressure to support access anytime from anywhere-while still protecting the enterprise network from intrusion.

Compliance

Sarbanes-Oxley, Gramm-Leach-Bliley, the Payment Card Industry Data Security Standard and the Health Insurance Portability and Accountability Act (HIPAA) are just a few of the legislated requirements that require companies to protect access to information. Compliance with relevant regulatory requirements not only requires organizations to take steps to protect access to information, it also encourages organizations to carefully log access and document compliance with regulatory requirements for protecting information.

Increased Sophistication of Security Attacks

Protecting the enterprise against illegal access to information is not only a requirement for business operations but also important for protecting brand value and corporate reputations. Hackers continue to develop sophisticated attacks that steal information and publicly batter corporate reputations.

Business Continuity

As has been seen recent in the recent past, natural disasters are usually totally unexpected and nobody ever plans for them until they occur. With these events, while there is inevitably some degree of social distancing there is an even greater need for communications. When people are affected, they want to be able to email and phone others not only in order to ensure that everyone is safe but also for the purposes of collaboration during a disaster. Having an effective means of instant but secure collaboration is key to organizations recovering from a disaster scenario and ensuring effective business continuity and viability. A successful business continuity approach needs to enable organizations to quickly recover from a disaster, connect all of their stakeholders and maintain productivity after the disaster has occurred. Unfortunately, more than 60% of businesses that undergo a catastrophe are unable to remain in business and close up shop within the next year following that disaster. Therefore, given these bleak statistics, organizations are realizing that business continuity planning should be factored into their overall remote access plans.

Companies strive to empower remote and mobile workers and enable their productivity without sacrificing security.

Implications for Business

Organizations need to develop a well-rounded approach to protecting remote access so they can:

- Ensure the security of information during transit
- Assure the identities of end-users requesting access to information
- Audit who is accessing which resources

At the same time, companies strive to empower remote and mobile workers and enable their productivity without sacrificing security.

Organizations also face the challenge of ensuring that remote and mobile user populations are able to securely tap into the corporate network so they can perform their jobs well no matter where they happen to be physically located. Companies try to constantly balance security and productivity, and deliver anytime, anywhere access to the internal private network via the Internet.

Internet-based VPNs can erase the administrative and financial headaches associated with traditional wide-area networks and allow remote and mobile users to be more productive. They can enhance productivity without negatively impacting the security and integrity of computer systems and data on the private company network-if the enterprise takes steps to strengthen access security.

Remote Access Considerations

In the not-too-distant past, information gathering was a function of time and resources. Today, a wealth of information is available to anyone with an Internet connection. The ubiquity of the Internet has leveled the playing field, allowing organizations of all sizes to compete successfully with one another. Real-time remote and mobile access was formerly the exclusive domain of larger firms with the IT infrastructure, budget and resources to ensure security. With new, innovative solutions, however, companies of all sizes can now take advantage of the Internet for secure connectivity.

A VPN allows an organization to use a public network-such as the Internet-to send and receive private data in a secure and private manner. The Internet Protocol Security (IPSec) standard was developed by the IETF and it defines a standard for providing network-layer authentication, access control, encryption, message integrity and replay protection for securing communications between network devices and applications. IPSec analyzes IP packets sent to-and-from a network interface, allowing those that match the configured security policy pass while discarding those packets that do not match the security policy. IPSec was used in early VPN implementations until SSL was developed as an alternative.

It is critical that organizations authenticate users to ensure that they are indeed who they claim to be before enabling VPN access.

Two Factor user Authentication

A token code that changes every 60 seconds means that the end-user's password changes every 60 seconds



While the need for site-to-site connectivity is well served by IPSec VPNs, the more complex challenge for organizations is the “high touch” endpoint management and dynamic access requirements of remote or mobile employees. IPSec VPNs are a good solution for a contained number of trusted users accessing the LAN from managed corporate PCs, and they are ideal for site-to-site connections where on-the-LAN experience is essential.

SSL is a proven network protocol for transmitting private documents via the Internet. It works by using a private key to encrypt data that's transferred over the SSL connection, and SSL is supported by all popular web browsers and is a leading standard for online transactions. SSL VPNs are a good solution for managing any number of users from different locations who use different devices and have diverse security privileges. They provide secure transport over the Internet without need to deploy and manage specialized client software, and they support highly flexible remote access using web-based interfaces on PCs as well as smart phones and PDAs.

SSL enables secure remote access to applications from any web browser and it enables superior administrative control, enhanced user flexibility and granular access control to enterprise resources by authorized users. SSL is easier to deploy and manage than IPSec, and it allows the enterprise to deliver secure remote access through any standards-based web browser.

With SSL VPNs, organizations can provide secure remote access to email and other applications to road warriors, employees working from home, traveling employees and users who rely on mobile devices while out of the office. SSL VPNs enable secure portal and extranet solutions as well as simplified access solutions for business partners.

Total Cost of Ownership

The total cost of ownership can be defined as the acquisition cost plus the cost of usability and maintenance over time. Since most organizations are cost-sensitive, the purchase price of a remote access VPN solution is a major consideration. Organizations also have to carefully evaluate the cost of usability and maintenance before selecting a secure VPN solution to ensure that the enterprise will not be burdened by excessive ongoing operational costs. The VPN solution needs to be able to be supported by existing resources and it has to be easy for end-users to gain remote access to ensure that the Total Cost of Ownership (TCO) remains low and productivity remains high.

Solutions that require users to install software on their PCs inevitably pose major support burdens on already-constrained IT resources. Non-technical users demand a solution that is simple to use and organizations often prefer to avoid IPSec VPNs and the cost and hassles of installing client software, configuring it, teaching employees how to use it and supporting them when they encounter difficulties.

User Views Of Passwords

Passwords are not enough to protect enterprise networks. Organizers of the InfoSecurity Europe trade show took an informal survey in London and found that:

- 71 percent of network users sampled said they would give up their passwords in exchange for a chocolate bar.
- On average, people have to remember four passwords, though one unlucky respondent had to remember 40.
- Those that used several passwords often wrote them down and hid them in a desk or in a document on their computer.
- 34 percent revealed the word or phrase they used when asked if it had anything to do with a pet or child's name.
- Family names, pets and sports teams were all used by those questioned to provide inspiration for a password.
- 80 percent said they were fed up with passwords and would like a better way to log into work computer systems.

Security

Still another important consideration is security. An open IPSec VPN tunnel is also a path into the corporate LAN. The tunnel itself is encrypted and secure, but that security is rendered **greatly weakened** if one end of the connection is open to the outside world (“split-tunneling”). Clearly in the case of a site-to-site connection it is reasonable to assume that the VPN connection is between two known entities, but this is not the case with remote users tunneling into the LAN. Today's remote access security concerns center around what can come in through the tunnel, taking advantage of VPN sessions that are often left open by users. For organizations large and small, even a minor security breach can mean anything from irreversible damage to brand reputation to the downfall of the business. While VPNs protect data during transmission, it is critical that the organizations authenticate users to ensure that they are indeed who they claim to be before enabling VPN access.

Securing the Enterprise

SSL VPNs take advantage not only of the Internet, but also of certain protocols intrinsic to its use. The SSL encryption protocol was originally developed for securing online financial transactions and is one of the foundations of web commerce. SSL is part of all standard web browsers, so the client software that initiates secure data transit is already on the PCs and mobile devices of end-users. Gartner has predicted that, “By 2008, SSL VPN networks will be the primary remote-access method for more than two-thirds of business teleworking employees, more than three-quarters of contractors and more than 90% of casual employee access.”

Organizations are trying to walk a fine line between effectively locking down sensitive information while making it very easy for non-technical remote and mobile end-users to utilize security best practices as they go about their jobs. An effective security solution needs to address both of these goals in order to achieve true secure remote and mobile access. Based on a Forrester Research survey, the top challenges for organizations when managing a growing mobile and remote workforce are ensuring strong levels of security while enabling seamless end-user productivity.

Limitations of Passwords

Passwords are insufficient for protecting access to SSL VPNs. While passwords are easy to create and use, and have proliferated throughout organizations over the years, they are surprisingly costly to the organization and have some key vulnerabilities that are increasingly encouraging organizations to move to strong authentication alternatives. Passwords are frequently stolen and prone to misuse. They are often written down or stored in desktop files for easy access by users, potentially exposing the organization to unwanted access by people who gain illegal access to stored passwords.

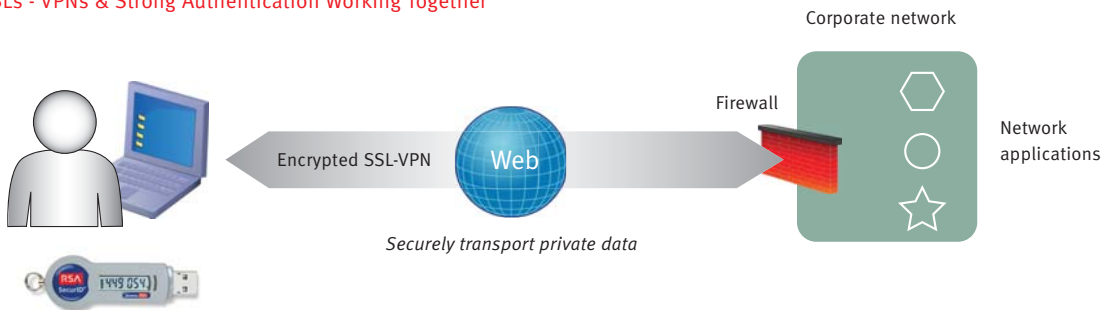
With passwords, it is very difficult for an organization to comply with regulatory requirements because of the inability to ensure that the right person is accessing requested information from a remote location. End-user frustration with passwords is becoming an increasing concern. Users want a more simple and consistent authentication method and, while they express frustration and management worries about weak security, the cost of managing these systems is

escalating out of control. Time is wasted as employees try to remember their passwords. Productivity is hurt each time a user gets locked out and has to call into the enterprise for assistance.

Supporting the overhead of these calls is expensive when you take into consideration the lost productivity of the employee and the expenses associated with responding to the user either through internal IT personnel or outsourced IT service providers. In many organizations, a third of all calls to the help desk are for password resets. Resetting passwords causes employees to waste time obtaining a new password and forces the organization to have the help desk staff in place to support a high volume of routine and avoidable user requests.

While employees express frustration with passwords and IT managers worry about weak security, the cost of managing passwords is escalating out of control. Time is wasted as employees try to remember their passwords, and productivity is hurt each time a user gets locked out and has to call into the help desk for assistance. The SSL VPN is exposed to greater vulnerability, and passwords do not provide sufficient assurance of identity to justify remote access to critical enterprise information through a VPN.

SSLs - VPNs & Strong Authentication Working Together



Establishing a trusted identity

The “Layered Security” approach

- Strong authentication is enforced before the the VPN is established.
- It can easily be added as additional layer of authentication (e.g. PKI / AD / LDAP)
- Endpoint security posture can and should be assessed before the VPN is established

A Secure Remote Access Solution

With strong authentication, the end user is asked for two-factors to identify themselves and the end result is that each user's identity is properly validated before they are provided access to the SSL VPN. Any organization willing to go through the effort of setting up a VPN environment to effectively protect the data during transit should take the extra step to ensure that the users who authenticate to the VPN are in fact who they claim to be. Two-factor authentication provides a layered approach to securing remote access where strong authentication is enforced and the endpoint security posture is properly assessed before the VPN is established.

Organizations can deploy the RSA SecurID® authentication solution to provide secure remote access for SSL VPNs. Remote users enter something they know-their personal identification number (PIN)- and something they have-the constantly changing token code on a RSA SecurID hardware or software authenticator. RSA Authentication Manager can be deployed centrally to power strong authentication for the RSA SecurID solution, or organizations can deploy the RSA SecurID Appliance to benefit from an integrated, rack-mountable hardware appliance format.



RSA SecurID® Form Factors

A Continual Trust Model

RSA's Identity Assurance portfolio extends user authentication from a single security measure to a continual trust model that is the basis of how an identity is used and what it can do. Trusted identities managed by RSA bring confidence to everyday transactions and support new business models by providing secure access for employees, customers and partners while striking the right balance between risk, cost and convenience. RSA's Identity Assurance solutions apply appropriate access controls that mitigate risk according to the value and criticality of the data, application, identity or transaction.

Access is granted to an SSL VPN only when the user has entered a valid RSA SecurID passcode; otherwise access is denied. Once the user's identity is assured, the authorization framework takes over, further limiting and restricting access to only those resources that are allowed. With RSA two-factor authentication solutions, organizations can empower workforce mobility and support both telecommuters and road warriors concurrently using the same physical device. Productivity is increased by offering anywhere, anytime access and employees can respond faster to business demands by having ready access to secure network resources. This solution also helps organizations incorporate best practices for compliance with regulatory requirements for protecting information.

A major practical advantage of SSL VPNs is that they do not need any client software to be installed and maintained on end-user PCs, and that SSL VPNs can be accessed from any public wireless access point. However, while SSL VPNs make it easy for more end-users to connect from anywhere the enterprise can be potentially vulnerable to security attacks because users may be coming in from unmanaged and less trusted PCs. While SSL VPNs provide encryption to ensure the confidentiality and integrity of data at rest or in transit, there is no guarantee that the user's identity is in fact valid-and it is possible that the data may still end up in the wrong hands.

Functional Requirements

RSA SecurID authentication was designed to secure remote access for remote and mobile employees. Remote users just enter their PIN and the constantly changing code on their RSA SecurID authenticator and gain network access as if their PCs were physically connected to the corporate network.

RSA offers RSA SecurID Authenticators in a wide variety of form factors, and also offers software-based authenticators that allow remote users to access the network using personal devices such as PDAs and smart phones. Users no longer have to remember often-incomprehensible passwords and can easily authenticate to the network and establish an encrypted tunnel using SSL. The solution is easily integrated into existing security infrastructure and can leverage existing account databases so the organization can augment its security posture and enable secure remote access very quickly.

Total Cost of Ownership

The RSA SSL VPN two-factor authentication solution is priced to accommodate the needs and budgets of any organization, large or small. The RSA SecurID authenticators avoid the cost and nuisance of resetting passwords and provide far greater security. Users no longer have to remember obtuse, complicated passwords that they will most likely want to write down, which potentially hinders information security and exposes the enterprise to attack. Authorized users just key-in their PINs and the current token code and once they are authenticated they can conduct their business online.

With RSA's two-factor authentication solutions, you avoid the cost of supporting users who have lost or forgotten their passwords, and you establish a single identity per user that can be applied across multiple applications. Granting access to a new user is as simple as adding their name, credentials and access controls or leveraging existing user directories. No further configurations need to take place, and a simple user activation process can be quickly carried out in order to issue a new SecurID token.

Organizations can meet remote access needs for both today and tomorrow by deploying RSA SecurID Authentication solutions for SSL VPNs.

Security

SSL uses strong encryption, and is a field-tested global standard for sensitive transactions. RSA two-factor authentication solutions protect SSL tunnels by allowing the organization to ensure that the person accessing the network is indeed who that person claims to be. Two-factor authentication can be integrated with policy enforcement, and organizations can centrally define policies that are applied to user groups. Organizations can leverage existing user account directories and endpoint security implementations while securing remote and mobile access to the enterprise.

Credential Management

An important consideration of an effective Identity Assurance solution is its ability to assign, revoke and otherwise manage the credentials that are issued to users. RSA® Credential Manager, a core component of RSA's Identity Assurance portfolio, provides full lifecycle management of RSA SecurID credentials. Offered as a feature of RSA® Authentication Manager, it centrally administers the deployment of RSA SecurID tokens and defines lifecycle policy. RSA Credential Manager also contains tools that both speed the setup and automation of workflows, and enable users to self-manage many aspects of their day-to-day token use. With RSA Credential Manager the entire deployment process – including populating the database and issuance of tokens – is fully automated.

Reporting

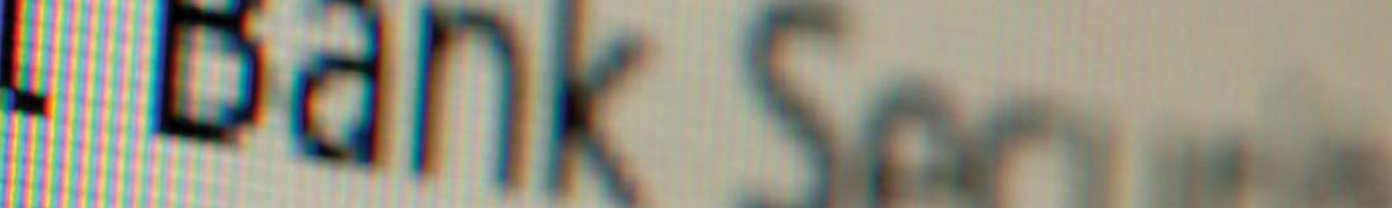
For both compliance and security reasons, it is important for organizations to be able to monitor and report on user activity and system usage. RSA Authentication Manager provides a vast array of standard reports and allows users to generate custom reports. Where there is a need for a more robust security information and event management system, RSA SecurID event data can be provided to the RSA enVision™ platform, a market-proven leader in transforming enterprise-wide data into automated compliance and security information.


Scalability

Organizations can meet remote access needs for both today and tomorrow by deploying RSA SecurID Authentication solutions for SSL VPNs. RSA's two-factor authentication solutions support cost-effective scalability so you can easily add new users as well, making the overall process very simple and concise.

Summary

RSA provides a compelling security solution that is flexible, simple to administer and very robust. RSA's strong, two-factor authentication technology has been embraced by thousands of companies and is used by millions of users worldwide. RSA SecurID two-factor authentication solutions allow organizations to secure SSL VPNs and enable easy-to-use and secure remote and mobile access to enterprise applications and information. Organizations can securely deploy SSL VPNs and protect access to information by implementing RSA SecurID solutions, and they can collect, analyze and correlate data from VPN platforms and other network devices using RSA enVision. Solutions from RSA allow organizations to securely and cost-effectively deploy SSL VPNs while protecting enterprise information and ensuring that remote users are centrally authenticated before being granted access to enterprise information via a SSL VPN.





RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2006-2008 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, SecurID, enVision, LogSmart and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

SSLVPN SB 0308



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com