



SafeEnterprise™ SSL iGate

Managing Central Access to Resources with VPX Technology

Introduction

SSL is a well-established, high performing and secure technology for Internet transactions. The strength of SSL lies in a reliable key exchange mechanism and strong encryption of the transmitted data. SSL is used in all ecommerce transactions and is the easiest Internet encryption technology to use and implement. SSL has typically only been used for Web based transactions – limiting the power of SSL solutions to Web based applications.

SSL has been married with sophisticated access control to bring SSL VPN's to market. SSL VPNs offer the lowest operating costs, least number of headaches and lowest user frustrations of any remote access solution. SSL VPNs also provide better overall security and, with optional integrated two-factor authentication, protect against the growing types of threats organizations face in the Internet connected and Web enabled world.

SafeNet takes SSL VPN security to the next level by offering the ability to support web and legacy applications all through one interface with VPX.

VPX

VPX stands for “Virtual Private anything” – the next generation of secure remote access. VPX technology from SafeNet harnesses the power, security and ease of use of SSL to secure client server applications and extend the ease of use of remote access to web based applications to more traditional client server applications such as Microsoft Outlook, Terminal Services, Telnet and Citrix. Leading CRM and ERP packages like Peoplesoft, Siebel, and SAP are supported in a client server or Web mode.

With SafeNet's VPX technology you can provide secure remote access anywhere that the user can access the Internet for non-Web based applications – but still using the tried and tested security of SSL. Remote access for non-Web based applications has been traditionally provided by IPSec technology.

SafeNet's VPX technology securely takes the protocols and ports that a particular client server application uses and redirects them over SSL. VPX technology is different from IPSec VPN technology because IPSec VPNs make a connection at the network layer to accomplish the same goal.

The SafeNet VPX technology securely creates independently encrypted and authenticated tunnels between the individual client side applications and the network application server. This technology works with any TCP based application. There are tremendous security benefits and usability benefits over alternative

solutions that VPX technology provides. These benefits are:

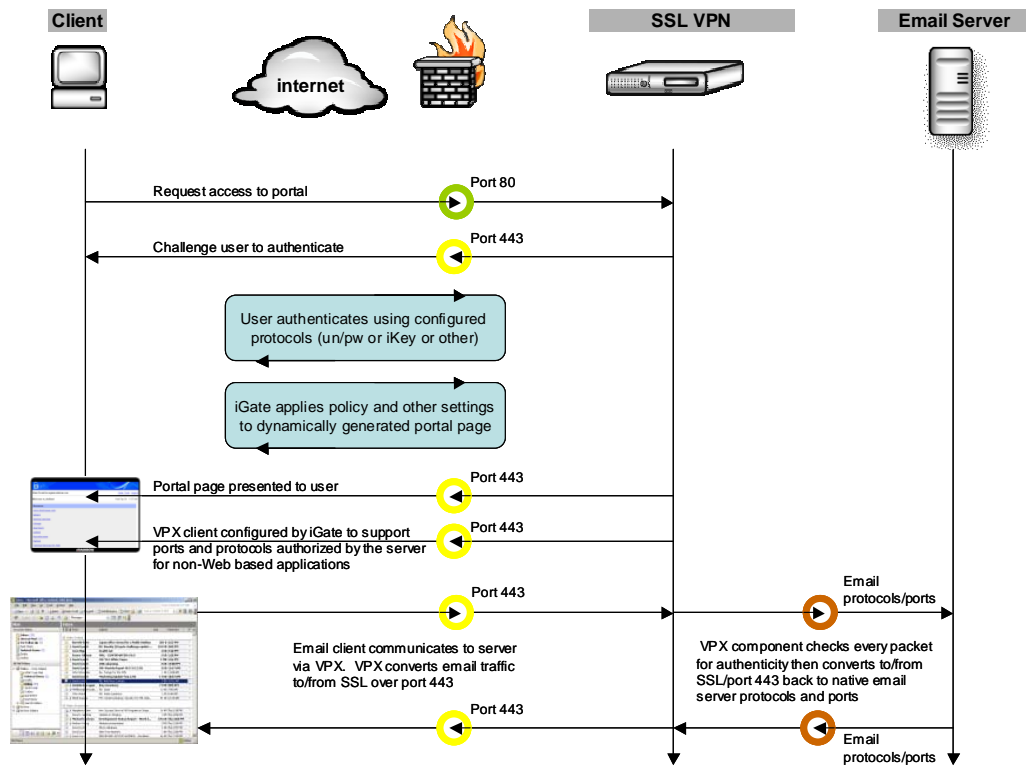
- Installation and maintenance of VPN software is not required. An applet is pushed down automatically when the session starts
- VPX doesn't require changes to your firewall
- Application servers do not need to be directly connected to the Internet
- Clients can be behind personal firewalls, NAT devices or other gateways – and still get secure access to the applications
- Networks are not bridged – so network level viruses and other potentially harmful software and hacks are simply thwarted from ever reaching the remote network.

VPX: How it Works

Because your application servers retain private IP addresses (NAT) and private domain names, they are protected from direct access from the Internet. However, your users' notebook computers or home computers need to be configured to access these resources as if they were directly on the corporate network – you don't want a solution where traveling salespeople have to run different profiles or have to reconfigure their email software each time they travel. The VPX solution takes care of this problem in a completely user-friendly way – requiring no configuration or changes by the user.

The diagram below shows the steps taken between the client and the application server:

1. The client securely connects and authenticates to the SafeEnterprise SSL iGate appliance.
2. This device creates a secure SSL session between itself and the client.
3. The client then initiates the VPX connection software – which is run in the portal page and delivered to any machine securely by SafeEnterprise SSL iGate.
4. The VPX software configures the client application (Ex: Microsoft Outlook) to communicate with the VPX software instead of the email server. This allows the client application and the user to remain unaware of any changes or complex configuration issues.
5. The client application then starts to communicate with the application server. VPX software grabs the protocols and traffic and converts it to SSL while adding additional information to the packets needed to communicate with the appliance. This information is securely transmitted over the Internet over SSL.
6. SafeEnterprise SSL iGate performs the same operation but in reverse; SafeEnterprise SSL iGate checks that each packet is coming from an authentic client and then converts the SSL packets back into the original protocols for the internally protected application servers.



VPX also adds the ability to provide “intervention less” configuration of the client machine. This ensures that client side applications can communicate remotely and securely with private application servers without being re-configured.

Two methods are supported and the administrator can select either. The first method is for the client side VPX applet to modify the local hosts file and instruct the client machine to forward its communications to a particular server to the VPX client instead. This way the client application does not need to be reconfigured. For example – a remote and private email server might have the address email.company.com and a private IP address. The VPX applet will modify the hosts file when it initiates so that traffic for email.company.com is routed to the VPX software instead. When the session terminates or the user logs out – the hosts file is restored to its original setting so that when the user is back in the corporate office the client application will communicate normally to the application server. The second method supported by SafeEnterprise SSL iGate VPX is very similar – but requires publication of private domain names on a DNS with pointers back to local host (note: it is only the domain name that is published – not the internal and private IP address). In other words – DNS entries must be made for email.company.com where the registered IP address is a local host address. In this way – when client machines are remote and connected to the Internet – the client application resolves the application server to the VPX client instead. This method relieves the VPX client from modifying the host file in circumstances where that is not possible.

SafeNet SafeEnterprise SSL iGate and SafeNet iKey

The SafeEnterprise SSL iGate SSL VPN solution performs high performance encryption with award winning hardware accelerated SSL processing built in to the product. Encryption protocols and security mechanisms are second to none. SafeNet believes that for complete application and user security that two-factor authentication is also required. SafeNet is the leading provider of secure two-factor

authentication USB token devices – and this technology is built in to the SafeEnterprise SSL iGate for customers that choose to deploy them.

With SafeNet iKey-based authentication, administrators have the confidence that accounts are not being duplicated or compromised by social attacks. When SafeNet iKeys are used for user authentication every packet that is transmitted is secured by technology much superior to username and password. Additionally, there is no concern about people forgetting to log off; when the iKey is removed from the system all open sessions and connections are terminated.

Summary

SSL VPNs offer a low cost, easy to deploy technology that is ideal for traveling employees or business partners that need access to a limited application set. VPX offers an easy way to use client-server based applications over SSL as if they were in the office. SafeNet's SafeEnterprise SSL iGate is the leading SSL VPN in the SSL VPN space because of SafeNet's extensive SSL background and authentication leadership. For more information on the SafeEnterprise SSL iGate visit:

<http://www.safenet-inc.com/products/igate/igate.asp>

=

SafeNet Overview

SafeNet, Inc. (NASDAQ: SFNT), a leading provider of private and public network security solutions, has set the industry standard for VPN technology and secure business communications and offers the only encryption platform for both WAN and VPN networks. With more than 20 years experience in developing, deploying, and managing network security systems for the most security-conscious government, financial institutions, and large enterprise organizations around the world, SafeNet's proven technology has emerged as the de facto industry standard for VPNs. SafeNet is the single source vendor for WAN and VPN security solutions teamed with an easy and low-cost migration path to a broad range of VPN products. SafeNet security solutions, based on SecureIP Technology™, and part of the CGX Security Platform, have become the products of choice for leading Internet infrastructure manufacturers, service providers, and security vendors. Securing the infrastructure of today's e-business communications as well as leading the way in government Homeland and classified data security, SafeNet has opened new markets for interoperable, secure, and deployable VPN communications. Commercial customers include Texas Instruments, Microsoft, Samsung, Centillium Communications, ARM, and Cisco Systems. Government, financial, and large enterprise customers include the National Security Agency, Federal Bureau of Investigation, U.S. Postal Service, U.S. Department of Defense, U.S. Internal Revenue Service, Social Security Administration, Bank of America, Eastman Kodak, Hewlett-Packard, and Motorola. For more information, visit <http://www.safenet-inc.com/>.



www.safenet-inc.com

Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 eMail: info@safenet-inc.com

Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail info@safenet-inc.com
Website www.safenet-inc.com

© 2004 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc. No part of this document may be reproduced in any form without prior written approval by SafeNet. SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The opinions expressed herein are subject to change without notice.

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111
India +91 11 26917538
Japan +81 3 5719 2731
Japan(Tokyo) +81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (1) +65 6274 2794
Singapore (2) +65 6297 6196
Taiwan +886 2 6630 9388
UK +44 1932 579200
UK (Basingstoke) +44 1256 345900
U.S. (Massachusetts) +1 978.539.4800
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California) +1 949.450.7300
U.S. (Santa Clara, California) +1 408.855.6000
U.S. (Torrance, California) +1 310.533.8100

Distributors and resellers
located worldwide.