

White Paper

SSL VPN
Software
Solution
SWANStor

AreaBe, Incorporated
San Jose, CA

<http://www.areabe.com>
ussales@areabe.com

Copyright© AreaBe, Inc 2003 All right reserved.



SSL-VPN and SWANStor Ever-Increasing Importance of Computer Security

Introduction

With the evolution of information technology (IT), business resources are becoming more digitalized. Today, business resources are accessible from the public more than ever and are now a crucial element of a successful business. However, security management of business resources is becoming more difficult to maintain and manage. The objective of any security management system is to deny any unauthorized external access and protecting private data shared over the public. The security system should also be able to grant certain access levels or privileges to each trusted user while the user can safely access the specified contents externally. In addition, it is important to reduce the overhead and costs of maintaining a security system.

Network and VPN

One of the remote access solutions to access internal business resources is the use of VPN (Virtual Private Network). Private networking that is conducted over a physically separated line is becoming increasingly “virtual” due to its high operational costs. It is becoming “virtual” in the sense of that these physically separated networks are migrating to use the public, shared infrastructure, due to the low operational costs, but are logically separated from other networks.

There are two main types of VPN on the Internet.

The first type is called “Network Type VPN.” Network Type VPN creates secure point-to-point connections between fixed sites. One type of Network Type VPN is IPSec-VPN. IPSec-VPN can connect sites through an encrypted IP tunnel. Another type of Network Type VPN is IP-VPN. IP-VPN, in addition to using a secured pipe, can also provide guaranteed quality of service.

The second type is called “Access Type VPN.” Access Type VPN allows access from remote sites using secure connections and this is the most important aspect for Access Type VPN.

From a technological point of view, the “Access Type VPN” and “Network Type VPN” are not different. Some “Access Type VPN” products use IPSec-VPN technology that requires installation of special software on the clients’ devices.

Issues with IPSec-VPN

IPSec-VPN provides a kind of network that the companies’ internal network is extending to the external device, such as a PC, through VPN tunnels. Therefore, the external PC can access any internal resource.

Although this seems very convenient, it is not suitable to apply an access policy such as an access filtering for internal resources depending on the login user account. Another issue with IPSec-VPN is that the external PC can possibly relay a third party's traffic. For these reasons, much consideration should be placed towards the clients' PCs.

What is SSL-VPN?

Many of the business resources today are constructed with Web based interfaces. Because of easy construction and management, web based business applications such as schedule management systems, customer management systems, email server access, WebDAV file access, etc. are becoming more mainstream. The web based business application is a target for SSL-VPN. The main idea of SSL-VPN is to provide safe access to web based business applications from the external network with a simple browser and without installing any special client software.

The SSL-VPN server forwards the web access request from the client's device just like a reverse-proxy server. Since the connection between the client's device and the server is encrypted by a SSL (Secure Socket Layer) session, there can be no privacy invasion by a third party on the information exchanged. The SSL-VPN Server can distinguish unauthorized requests/access from access devices by means of the login authentication process, which uses the combination of the access user account and password. In addition, SSL-VPN Server has the function to filter accessible business resources depending on the access user account. There is no possibility that the third party's traffic will be relayed, since the basis of the access is the browser.

SSL-VPN of SWANStor System

The SWANStor System is one of the available SSL-VPNs products and contains unique features that other SSL-VPN products do not provide.

The SWANStor System can coexist peacefully with any firewall and can maintain or enhance its security system. The SWANStor System can allow all inbound network ports at the firewall to be closed without interfering with the operation of the SWANStor System and user access.

Other VPN/SSL-VPN products are constructed as a single device and are placed within the firewall or DMZ (DeMilitarized Zone) area. These products require one or more ports on the firewall to be opened so that the VPN Server can access the companies' network when the device is placed within a DMZ area, or external users can access the VPN Server when the device is placed within the firewall. There is no doubt that opening a port for inbound traffic can create a security risk or "hole" because any open port will need additional configuration to deny unauthorized user access. Regardless of the firewall settings or its configuration, the VPN Server itself could be exploited in which internal resources are exposed and possibly subject to harm.

The SWANStor system, consist of a SWANStor Server and a SWANStor Gateway. Both the SWANStor Server and the SWANStor Gateway combined, carries out the equal function of an "SSL-VPN Server". The SWANStor Server can establish and maintain encrypted sessions with the SWANStor Gateway. The sessions between the SWANStor Gateway and the client can also be encrypted using SSL. Therefore, no other third party can eavesdrop on the users' traffic. Again, all incoming ports on the firewall can be closed because the SWANStor session is established from the SWANStor Server to the SWANStor Gateway. Even if the SWANStor Gateway system itself had been "hacked" into, it cannot be used to access SWANStor Server or the internal network due to its proprietary SWANStor session. The SWANStor Gateway never caches web contents nor does it contain sensitive information such as user names/passwords.

SWANStor System Configuration

In order to access the business resources through SWANStor, it is necessary for the access user to know the appropriate SWANStor Gateway address. Once the user accesses the SWANStor Gateway with a browser, the server name, login name, and the password are requested. Access to the companies' resources is possible only if the SWANStor System authorizes the access user after entering the respective values in the fields mentioned above.

From the perspective of the access user, the SWANStor Gateway itself may look like the companies business resources, though in reality, these resources are deployed behind the SWANStor system and are protected by the corporate firewall.

It is possible for multiple SWANStor Servers to connect to a single SWANStor Gateway. The user's request will be redirected to the appropriate SWANStor Server via SWANStor Gateway using the server name that was requested during the login process. The SWANStor Server provides additional security by using a unique session ID that will be assigned to each individual user's session once the user has been successfully authorized. The session ID is a random number generated by the SWANStor Server. In addition, no third party can intercept the traffic between the SWANStor Server and the SWANStor Gateway because the traffic is encrypted in the same manner as SSL.

SWANStor and Access Control

SWANStor has the following three types of access controls:

First, users cannot access business resources through SWANStor unless the 4 tuple are supplied. The 4 tuple supplied are the SWANStor Gateway address, SWANStor Server name, user's login name, and the user's password. Additional standard authentication routines can also be performed using such standard authentication protocols such as LDAP, RADIUS, RSA SecurID, and WindowsNT (Windows version only).

Second, each access user can be classified into a group that defines which business resources that can be accessed. Therefore, the visible business resources can be divided between the users on the single SWANStor System, such as a catalog information site for vender A and another catalog information site for vendor B.

Third, SWANStor has an access level filtering feature that can control what web contents a user can access. For example, it may be wise to have an access control level specified if both partner company A and partner company B are using a shared web server but contain different web contents.

SWANStor and Security Management

All of the access control functions mentioned above are performed on the SWANStor Server. Any administrative configuration or environmental settings applied for the SWANStor Server are performed through the SWANStor ServerManager, which is a web based maintenance console. The SWANStor ServerManager cannot be accessed through the SWANStor Gateway, therefore the access control settings cannot be changed from a remote site.

All business resources, such as the SWANStor Server, web servers, and authentication servers, are deployed inside the firewall. All network ports may be closed on the firewall and no other sessions, other than the SWANStor session, are needed to access internal resources.

Although the SWANStor Gateway appears as the web server itself from the client's browser, the true role of the SWANStor Gateway is that it forwards the request to the appropriate SWANStor Server on behalf of the client.

There is no way for unintentional or unintended traffic to be sent out to the outside by the SWANStor System if a program like the Trojan horse was placed on the companies web server, because the SWANStor Server is designed to work passively. Any traffic from the SWANStor Server to the client is invoked only by the client's request. It is also possible to monitor access from the outside using the SWANStor Server's access log, and to filter out suspicious access from the inside to the outside with the proxy server and the firewall.

Conclusion

The SWANStor System that applies the SSL-VPN technology contains more advantages than any other available SSL-VPN product today from the security management point of view.

First, the SWANStor System can reduce the overhead on security administrators from any unwanted intrusion from the outside to any of the internal business resources because all of the direct access from the outside can be blocked by the firewall.

Second, the SWANStor System can possibly track down on any internal node(s) sending any suspicious traffic from the inside to the outside. Any suspicious outgoing traffic can be filtered at the proxy and the firewall by setting the access password on the proxy and by restricting the permitted port on the proxy and the firewall.

Third, it is possible to track down the point of attack by unknown "hacker" by placing everything except the SWANStor Gateway machine within the firewall. Installing the SWANStor System does not mean that security management is no longer necessary.

In summary, the SWANStor System provides a superior solution as a convenient and a secure means of remote access in which the user can enjoy the benefits of what SSL-VPN technology has to offer and security administrators can reduce their overhead allocated on the computer security management.

The logo for SWANStor, with "SWAN" in a bold, grey, sans-serif font and "Stor" in a bold, orange, sans-serif font.