SecureAge

SV3000 SSL VPN

SecureAge SV3000 SSL VPN is a reliable, easy-to-deploy remote access security solution that will put an end to all your frustration and concern. It leverages on the well-established SSL (Secure Sockets Layer) technology that gives you the most robust and integrated solutions to secure all the remote access to your corporate network.

Why is SecureAge SV3000 SSL VPN the Perfect Solution?

Application Layer Security

SecureAge SV3000 uses SSL as the underlying securityprotocol to prevent unauthorized users from accessing the enterprise networks or applications. SSL enables secure HTTPS sessions by securing data above the transport layer without interfering with the lower layer network services. HTTPS sessions, universally regarded as standard web traffic by firewalls and traffic filters, allow secure remote access to any enterprise networks or applications from any remote networks. Even if you are using a non-web protocol, SecureAge SV3000 is able to support application layer proxy via Java applet by channeling non-web protocols over secure SSL session..

Built-in High Availability (HA) and Failover Features

SecureAge SV3000 comes with built-in HA and failover features which ensure uninterrupted VPN access to the enterprise network. State information and data files are automatically replicated between a pair of SV3000 appliances. If the primary appliance fail, the lost sessions will be automatically re-established by the backup appliance. It saves your remote user the trouble of re-conneting all over again.

Comprehensive Digital Certificate Authentication with Advanced PKI Technology

SecureAge SV3000 is able to centrally manage PKI (Public Key Infrastructure) based digital certificates for all users and use them for secure authentication for enterprise applications and services. To boost security, SecureAge SV3000 also provides advanced PKI features like certificate revocation checking via Certificate Revocation Lists (CRLs) and real-time OCSP support. SecureAge SV3000 also supports smart card and USB token, encryption with unlimited key length RSA asymmetric key algorithm, and 128-bit RC4, 168-bit Triple-DES and 256-bit Aes symmet ric key encryption.

Clientless Secure Remote Access

SecureAge SV3000 is a clientless SSL VPN. Your IT administrators need not install and manage the complex IPSec VPN client for your users to enjoy secure remote access. All your users need is a standard web browser to connect to your corporate resources anytime and anywhere.Alternatively,SecureAge SV3000 also provides a client based solution which is self-sufficient in creating the secure SSL tunnel without any web browser support.

Robust Security Infrastructure

The robust security infrastructure of SecureAge SV3000 fully secures your remote access. It is protected with a fully harden OS that allows only SSL VPN traffic to pass through. It also comes with a built-in firewall that automatically blocks off any illegal attempt to access the internal network via the VPN gateway. Developed with advance technology, it is protected from buffer overflow bug that plagues other network security appliances. Unlike other SSL VPN vendors, our solution does not rely on third party software like OpenSSL. OpenSSL is known for its security flaws which lead to either a denial-of-service attack or system break-in by an unauthenticated, remote attacker from the Internet. Frequent security patches to fix the various security loopholes are necessary to sustain the security strength and can be a great hassle to your IT administrators in the long run. But by using SecureAge SV3000 with its fully owned and developed SSL library, all the security vulnerabilities faced by OpenSSL is overcome.

Secure Remote Access Made Easy

SecureAge SV3000 provides secure remote access in one industrial grade appliance. It can be rapidly deployed and integrated into company's network without modifying the existing application servers and security mechanisms. Key security features and security elements like authentication, policy and encryption are bundled into the appliance for fast and reliable deployment. This therefore makes SecureAge SV3000 SSL VPN appliance an easy to manage and maintain solution

More Powerful Than IPSec VPNs

Organizations deploying IPSec VPNs have to shoulder the burdens of resolving problems like firewall blockage, NAT (Network Address Translation), limited remotedevice support,tedious software installation and maintenance and the inability to access reliably to confidential information from anywhere, using any device. But organizations will be free from all these burdens once they use SecureAge SV3000 SSL VPN. SecureAge SV3000 operates over a single SSL tunnel which will greatly improve the overall computational performance and access control. A single SSL tunnel means that only one-time authentication per user is needed and the user information is not stored on local machine which can lead to impersonation attack. It also trans lates to less resources being consumed on the SSL VPN server for multiple applications access.

Web-based Administrative Control

With SecureAge SV3000, managing user authentication and authorization privileges is now a bliss to your IT administrators. Managing access can now be done centrally and remotely for all your users. SecureAge SV3000 provides dynamic rules based access which allows your administrators to define restricted levels of access or even deny access altogether based on user parameters such as time of access, or type of authentication being used. SecureAge SV3000 also allows every application to have their different authentication mechanisms. Your administrators can have the flexibility of assigning different users with password, authentication token or digital certificate for accessing information ranging from routine to highly confidential in nature.

By using SecureAge SV3000, your IT administrators can now track, audit and generate reports of the user activities, session and activation logs via internal or external Syslog server. They can also monitor the health of the overal lsystem using a web-based real time view of the system state and connection statistics.

Key Features

. Provide role based access control rules like the user role, application role as well as user role and application role access mapping.
. Support external LDAP, Radius and Microsoft AD for user grouping and user authentication.
. Support external PKI / CA for certificate based authentication and certificate validity checking.
. Support user definable plug-in module for customized user authentication.
. Provide SSO (single-sign-on) module to support single-sign-on to applications that require additional authenti cation.
. Provide optional embedded Certificate Authority module.
. Support up to 1000 concurrent users.
. Support more than 100 Mbps network throughput rate.
. Gigabits network ready.
. Require only single port access to SSL VPN (443) from external network.
. Support client and server authentication through digital certificates.
. Enable optional built-in PKI/CA in the SSL VPN gateway to provide a total PKI based authentication solution.
. Provide support for default client side SSL engine as well as customized SSL engine with advance and/or propri etary encryption algorithms.
. Standard 1U rack mountable chassis.

SecureAge Technology Pte Ltd
20 Ayer Rajah Crescent #09-13
Technopreneur Centre Singapore 139964
Tel: (65) 6873 3710 Fax: (65) 6234 4992
URL: http://www.secureage.com
Email: contactus@secureage.com

SecureAge