

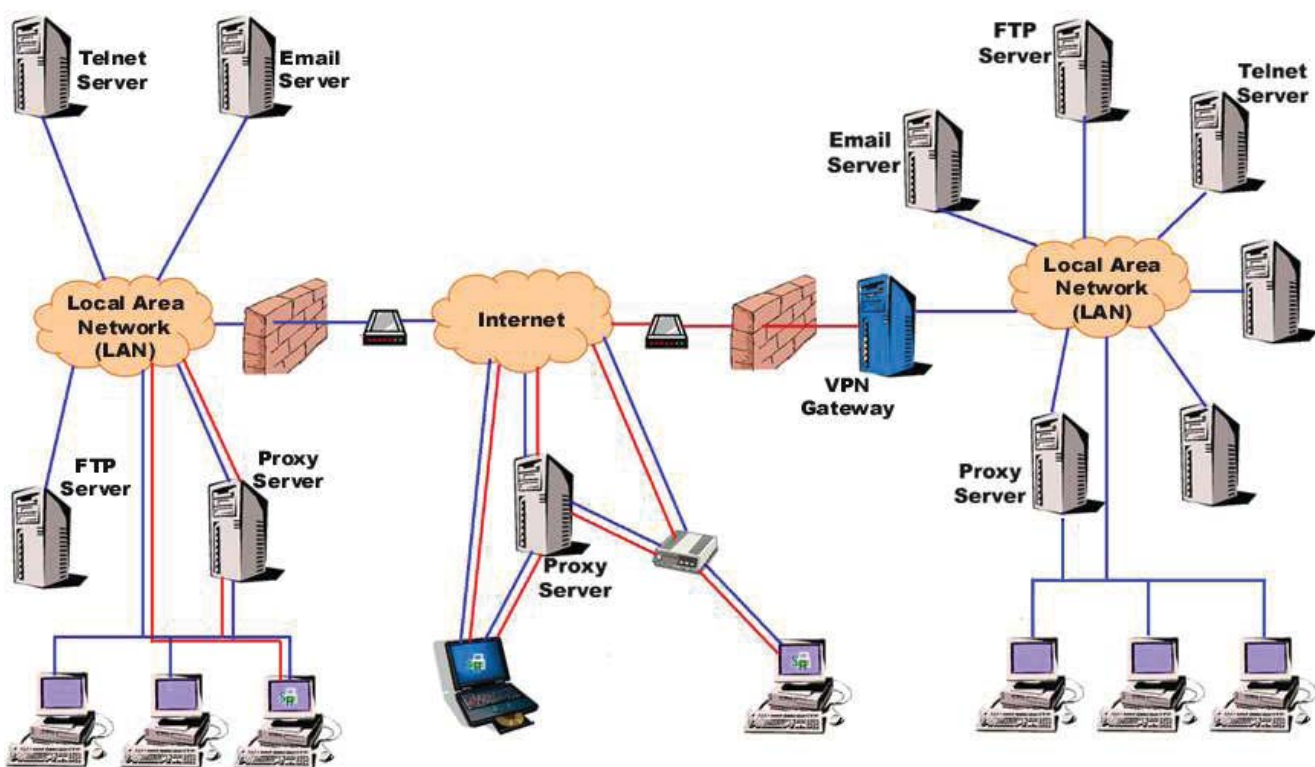
SecureAge

SA SecureAccess

VPN (Virtual Private Network) is undoubtedly a fast and cost effective way of allowing remote access to various locations for your employees, business partners and customers worldwide. Currently, employees who are always on the move can easily access company's critical information anytime and anywhere. However, its effectiveness does not necessarily mean it is secured. By using a password does not really mean that you are highly protected. As long as information can be readily accessed from outside your office, you are at risks. Any unauthorized person can easily access your customer records, sales proposals, corporate contracts, product specifications, legal documents and credit card information over your corporate network. Threats are practically lurking everywhere. But these threats can be overcome by using SecureAge SA SecureAccess. It will enhance the security of your VPN by providing users' identification, verification of communications and comprehensive security management of the user's identities. By implementing our SA SecureAccess into your system, you can be assured of high-level authorization, data privacy, data integrity and non-repudiation when securing your ebusiness applications.

Product Description

SA SecureAccess establishes a full-strength secure channel for your employees, business partners and customers to access and exchange critical information over your corporate network. Security is built over our SecureAge infrastructure which allows integrated access control. It also provides fine-grain access control which allows selective access to information. Strong encryption algorithms and authentication features within SA SecureAccess Client, SecureAge, not only enables privacy, but also guarantees the authenticity of users and integrity of the data. Its scalability function is able to size the security management according to the number of users and devices found in the networks. This will cut down the administrative nightmare, reducing the administrative overheads and allowing the administrator to concentrate more on their core business. All in all, SA SecureAccess promises to secure your VPN by providing full-strength authentication, data privacy, data integrity and non-repudiation.



SA SecureAccess is able to accurately identify both users and devices by assigning unique identity to all VPN users. To establish a secure, authenticated VPN connection, Digital Certificates are used to identify users with certainty. The good thing about these certificates is that they do not transmit user passwords across the Internet or storing them unprotected on network servers. This prevents potential hackers from stealing the user's password. However, there are still room. improvement pertaining to the security strength of Digital Certificates. Their security strength can be further fortified by using a physical token or smart card as a form of user authentication. Key pairs can be generated and safely stored on the card. This makes it impossible for private keys to be accessed or copied to a server by unauthorized users.

Encryption can ensure that the transmitted information is not eavesdropped or tampered with. Once the data is being encrypted by the sender, only the intended receiver who holds the private key can decrypt the data. Basically, SA SecureAccess offers you the option of integration with Public Key Infrastructure (PKI) to greatly enhance the security strength of your VPN. It is imperative to take advantage of this integration capability as a simple username or password is really insufficient to secure your VPN and allowing you to enjoy the full benefits of VPN.

But how can you ensure non-repudiation when there is no paper evidence to prove that the online transactions actually did take place? SA SecureAccess, with its integrated PKI support, can issue proof of the actual transactions being conducted between two authorized people. It provides a reliable environment with fundamental protection to communications by creating and managing trusted electronic identities, verifying the integrity of transmitted data and ensuring enforceability of electronic contracts.

Most companies secure their Internet Protocol (IP) traffic as a mean to safeguard their corporate network. As a result, some mobile professionals may face the problem of accessing their corporate network via private IP when they are overseas. This is especially true for those using wireless Local Area Network (LAN). In order for private IP to access the corporate network, it needs to go through Network Access Translation (NAT) for translating IP traffic. However, some generic VPN traffic is not translatable by the remote network NAT and the user is thus blocked from accessing their corporate network. This problem can be resolved by using SecureAge® SA SecureAccess. It has no problem working with private IP since its security and integrity protections are provided at the application layer application layer. Therefore, SA SecureAccess is not affected by NAT.

Some mobile professionals may also encounter problem when they attempt to access their corporate network in another company who has its own firewall. This is largely because firewalls restrict access to the Internet, for example, to only allow web and email traffic. By default, most VPN traffic are automatically blocked by firewalls. However, by using SA SecureAccess, you can easily access your corporate network from within other firewalls as it allows VPN traffic to piggyback on standard protocol like the web traffic.

Key Features

- Enables secure remote access to existing services such as telnet, email, www and ftp.
- Enables secure Business-to-Business transactions.
- Fully compatible with remote access from private IP address using Network Address Translation (NAT).
- No client reconfiguration of firewall is necessary.
- Strongest security using 1024-bit public key and 168-bit encryption algorithms.
- Integrated PKI support.
- Support flexible user authentication based on:
 - i. Certificate.
 - ii. UID/Password.
 - iii. Biometrics and Physical Tokens.
 - iv. Plug-ins.
- Role based integrated access control to allow users to access only services that they are authorized to use.
- Java based, multi-platform support.
- Provides web based remote administration.