



**Secure
Resilient
Networks**

November 2008

Overview

Security

By: Harri Chiba
Sales Manager, CI-Net Ltd

Security Overview

One of the most important requirements for almost all organisations is the ability for employees, no matter where they are, to securely access corporate IT systems and data.

Historically this was achieved using private connectivity between head office and regional offices. This had two drawbacks, firstly cost and secondly that this could not cater for employees that were off site (roaming). This inflexible approach forced companies to maintain multiple access methods often consisting of expensive fixed links and dial in services.

Recently the majority of UK businesses are choosing Virtual Private Networks (VPN) instead of using private point to point circuits to access their corporate data. Using VPN's to enable connectivity to all company sites, either over the internet or a provider's shared infrastructure (MPLS, IPVPN, NetEquip, IPClear etc) can introduce huge risks if not carefully managed.

It is crucial that regardless of the underlying transport network, there is end to end encryption of your Data using IPSec VPN or SSL VPN

IPSEC VPN

Internet Protocol Security (IPSec) provides an encrypted secure set of protocols developed by the IETF to support the secure exchange of packets (data / traffic) at the IP layer. IPSec has been used widely in the deployment and implementation of VPNs.

IPSec supports two encryption modes: **Transport** and **Tunnel**. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. Once transmitted, an IPSec-compliant device on the receiving end decrypts each packet. CI-Net employs the use of Tunnel mode IPSEC VPN.

For IPSec to work, the sending and receiving devices must share what's called a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using the digital certificates.

Internet Protocol Security (IPSec) provides enhanced security features, such as better encryption algorithms and more comprehensive authentication.

Typically IPSec VPN's are deployed for router to router environments; they offer a standard that allows different vendors equipment to communicate securely.

A standard IPSec VPN deployment can be seen as securing a link between site A & B i.e. point to point, where traditional VPN's are meshed you find that traffic from site B destined for site C must



November 2008

be securely transmitted from site B to site A and then transmitted again from Site A to site C. CI-Net deploy a method of automatic meshing that negates this need (see Stonesoft Products).

SSL VPN- Netilla

SSL: SSL stands for Secure Socket Layer – this layer provides a secure communication connection to the Internet for such things as web browsing, email and Internet faxing, instant messaging and other data transfers. SSL uses a cryptographic system that uses two keys to encrypt data a public key known to everyone and a private or secret key known only to the recipient of the message. Many Web sites use the protocol to obtain confidential user information, such as credit card numbers. The URLs that require an SSL connection start with *https:* instead of *http*.

Typically SSL VPN's are employed to secure access from a single remote machine to an internal network. They are easy to use as they can be launched using a browser and familiar desktops or user interfaces can be displayed to the user to provide access to corporate resources.

AEP's Netilla Security Platform SSL VPN (NSP) helps companies satisfy one of their most pressing needs: Making business applications remotely available to employees and partners.

With the NSP, remote users can quickly and securely reach the varied resources found in today's IT environment, including Microsoft Outlook, Windows Terminal Servers and server-based applications, as well as client/server applications over an SSL tunnel.

The NSP is available in several classes designed to meet your organisation's capacity needs.

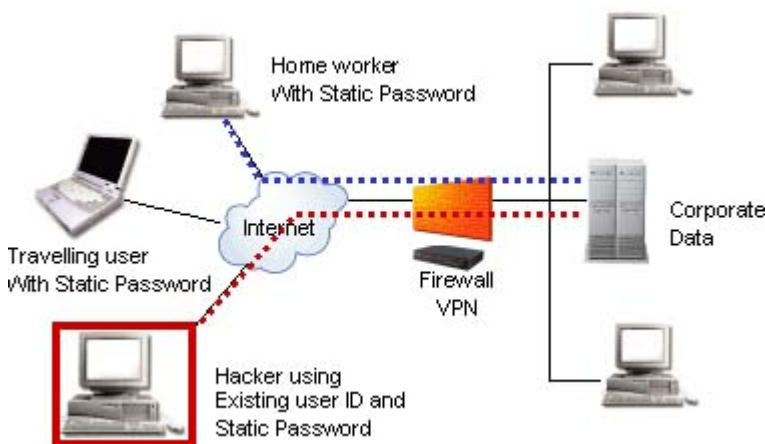
Additionally, the NSP with Federal Information Processing Standards (FIPS) support is designed to provide secure remote access to highly confidential data to meet the most stringent U.S., Canadian and U.K. security standards.

Vasco

Vasco provide a security device in the form of a token referred to as a DIGIPASS, this provides strong user authentication and e-Signatures. This device is compatible with more than 50 international vendors for e-Commerce, e-Banking, e-Networking and e-Government applications. The Digipass Pack provides what's called "two factor strong authentication" for any radius environment and is certified for many VASCO Ready Solution Partners. Two factor authentication is defined as something that you know and something that you have e.g. a PIN number that you know and a VASCO token to generate a number that changes every 30 seconds.

One of the biggest vulnerabilities in security that could allow network hackers easy access to corporate information is "User Authentication". A randomly generated pass-key which can be used as an additional method of identification minimises this risk, this is known as "Two Factor Authentication".

Home-workers, travellers and Internet users will all rely on VPN and firewall technology to enter corporate networks gaining access to sensitive resources. The Vasco token provides this secure authentication to enable access to these secure environments.



Within CI-Net solutions we often use Vasco tokens to secure SSL VPN connections. Because of the ability to launch an SSL VPN from any PC with a browser we advocate secure password entry to these systems using access based on Vasco tokens.

Stonesoft Products

StoneSoft are a company specialising in the provision of hardware giving users multi-linking and load balancing capabilities combined with firewall and management systems.

The StoneGate Management Centre forms the core of the StoneGate Platform, providing unified management for StoneGate Firewall, VPN, and Intruder Prevention System (IPS) solutions.

This management system enables the users to incorporate the following:

- Manage the security solution holistically
- Utilise shared network elements
- Benefit from shared logging, reporting, auditing, and other tools

The real benefits of the StoneGate management centre means that you don't require a separate management tool for each security device; they can all be managed centrally from one single management centre. This means you do not need to sacrifice manageability to use a "unified management" for systems that were not designed to be managed all together.



November 2008

Implementing this solution enables us to manage large infrastructures, providing the unique ability to roll back to previous configurations should the need arise and provides a remote management tool in the event that this is required.

Features

Unified configuration of security, networking, and resilient connectivity the advantage of this is to reduce complexity and increase security and service availability.

The security overview advantages provide unified tools for monitoring, reporting and incident handling.

The ability to remotely manage the configuration, backups, and upgrades for remote sites is a real advantage.

- Role-based administration feature allows the user to securely delegate management tasks.
- Meshed VPN topology

Benefits

- Increases in efficiency by saving time and money on everyday routines, especially in multi-site environments.
- Peace of mind in knowing that you always have visibility of the "big picture."
- Eliminates the need for security and networking professionals in remote sites with the ability to upgrade or recover your system in minutes or hours, rather than in days or weeks.
- Administrative resources are increased and management tasks are executed as efficiently as possible.
- Administrator accountability through auditing and strong user authentication makes it easier to comply with regulations.