

Application Note 2032

Secure VPNs—Using the Internet to provide Business Data Links

Low cost high performance virtual private networking over public and private networks using Network iQ™ routers and Network iQ™ encryption engines.

NOTE: Following the acquisition of the Network iQ product range from Teltrend, Inc., Allied Telesyn have renamed the Network iQ Router as the AR Router.

By utilising high performance dedicated encryption processor boards in combination with enhanced features on the popular Network iQ™ routers, Allied Telesyn now offers a secure virtual private networking (VPN) capability that is second to none in the wide area networking industry. Apart from allowing high level security implementations for the government and financial sectors this also provides for industry leading “real world” corporate networking over public networks such as the Internet. This allows substantial cost savings over traditional network connections. It also provides a future proofed architecture with strong links to market trends and standards.

Figure 1: Using the Internet to provide links between corporate business centres.

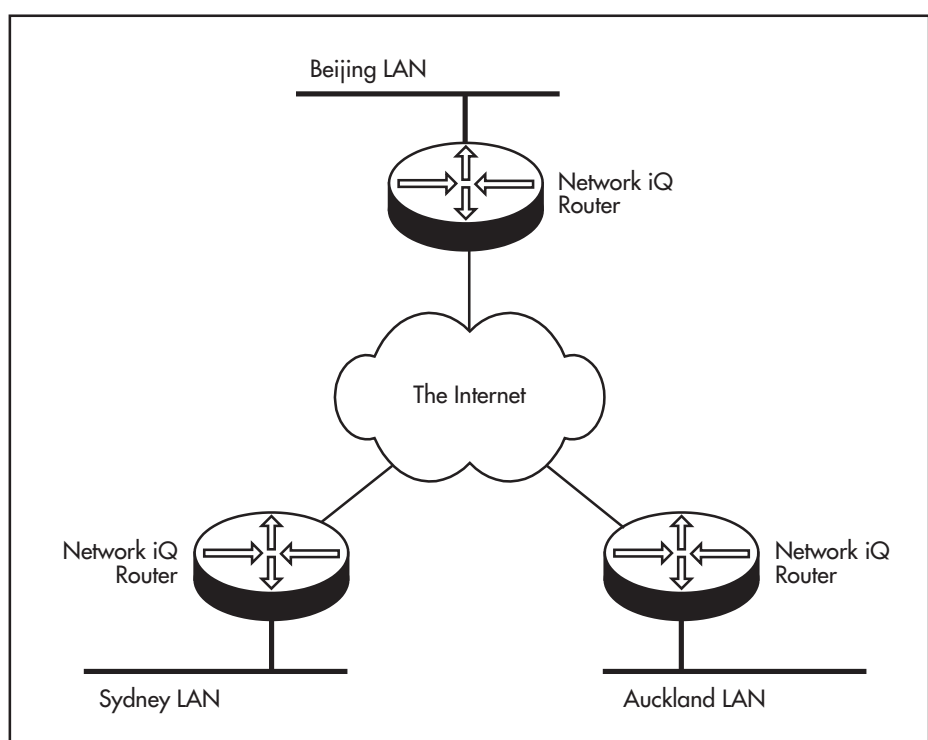
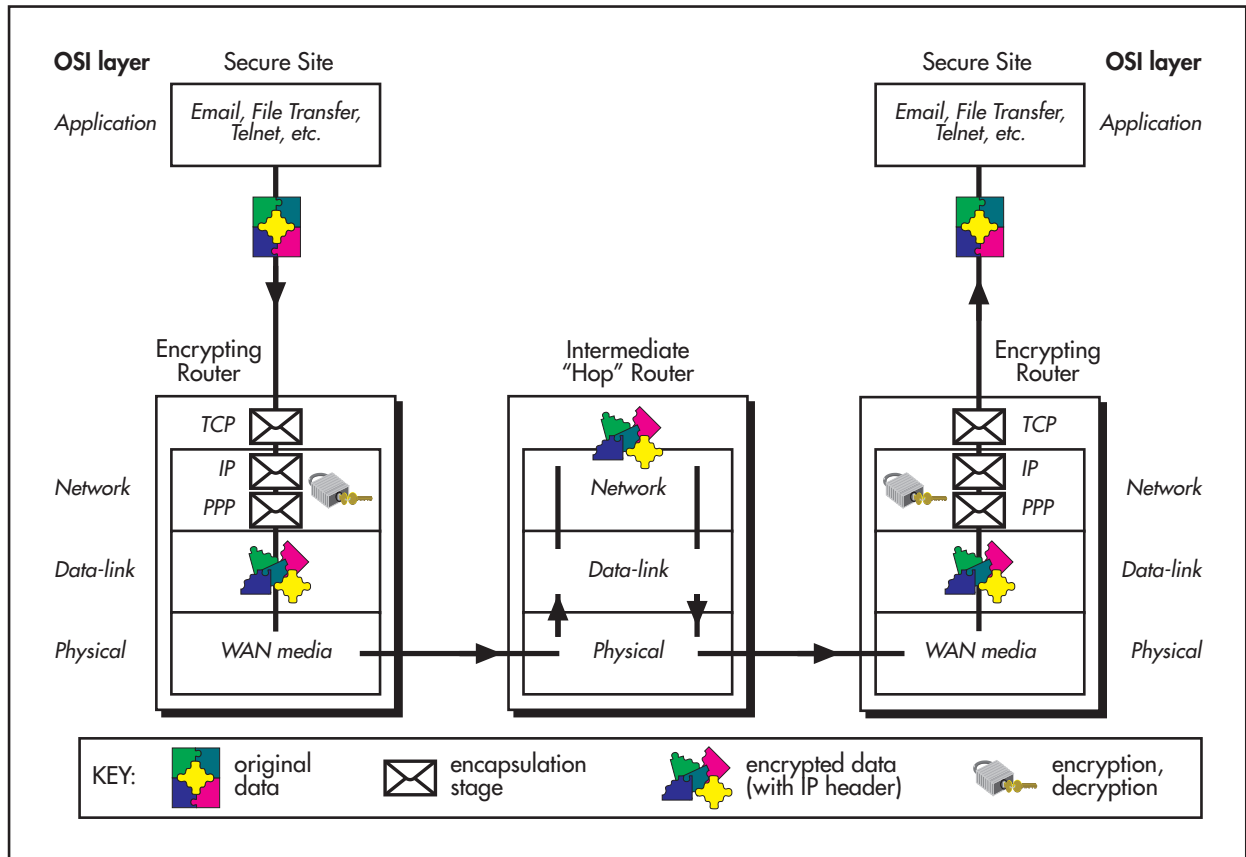


Figure 2: How payload encryption works.

As each packet is created by an application program it is then passed on to the various protocols in use, from there they are encrypted and passed out onto the network. From this point they are forwarded at each stage in their journey as encrypted IP packets. A copy of the source and destination IP address information is included in the packet header to allow intermediate devices to forward the packet. Upon reaching the destination this process is then reversed and the packets are delivered to the receiving host application program.



Background

Three ways to build Secure VPNs

For some time experienced network administrators and network designers have realised that implementing business solutions over public networks such as the Internet has not been a realistic option, particularly for companies requiring high performance or strong security. A second major barrier is that of implementation—even if there is a secure solution is it a practical one? Costs both up front and hidden arise in any technology implementation—how can these be minimised or avoided? A common source of hidden costs is that of administering the network equipment. Another is the future costs of upgrading and modifying the network to meet emerging needs. Currently network administrators and designers face three choices in building a secure network, these are also applicable in the case of building secure VPNs.

■ Option 1—Software running on a PC

The earliest players in the Secure VPN arena were companies offering additional features to their existing routing or security software programs. Apart from providing a reasonable low end option for smaller businesses

these companies have, and continue to help bring the concept of secure virtual private networking into general awareness. They have also helped to highlight the key issues associated with constructing secure VPNs in a business environment. When talking in terms of business solutions however, it has long been recognised that, apart from the obvious performance limitations, software based cryptographic implementations can prove to be seriously flawed in terms of security when attempting to provide encryption services such as the U.S. DES military standard. Despite claims that recent advances in technology overcome these difficulties it is widely acknowledged that DES encryption (and other methods like it) is not designed to be implemented as a software application.

■ Option 2—Additional Hardware Devices

Following closely behind the PC software companies a number of router and security product vendors began offering limited function Secure VPN services with reasonable success. These solutions are typically offered as a package or upgrade utilising 3rd party hardware encryption and compression devices to enhance standard routing products. While this appears to work, as it provides an encrypting facility, it also suffers from the disadvantages of cost and flexibility.

- Cost because there is the requirement to duplicate each network access device as well as (in most cases) each WAN link—this alone can double the installation costs! This is also an expensive option as it requires additional network management and offers little or no future proofing against changes both in industry standards and network requirements.
- Flexibility is also lost as network design and maintenance limitations are introduced by differences between the design and operation of the devices from two different manufacturers. This can be most painful in issues relating to configuration, device compatibility and change due to network evolution.

■ Option 3—Integrated Hardware

Very few vendors to date have demonstrated the ability to offer a viable product under this option. Allied Telesyn has seen this as the premium strategy particularly for mid and large size applications. Development and refining of the Total iQ™ product ranges have continued in parallel with that of manufacturers of the PC software option. Now, with Network iQ™ ENCO (encryption/compression) expansion modules running on Network iQ™ products, Allied Telesyn offers a flexible, highly integrated solution. This solution is hardware based and is designed specifically to meet the performance capabilities demanded by today's business environments. The Allied Telesyn offering provides protection both in terms of data security and future proofing in terms of business investment. This is achieved through the fully integrated 'by design' configuration utilising the elements that have made Network iQ™ routers an industry player in the wide area networking arena. Using hardware encryption devices helps to overcome performance limitations typical with PC software options. Running encryption hardware in a platform specifically designed for the purpose removes the cost and flexibility limitations of using additional 3rd party security devices. Thus by using Allied Telesyn products you can enjoy the best of both worlds!

Building a TCP/IP Security Architecture

Secure Virtual Private Networks can be built over the Internet using the standards based Network iQ™ router TCP/IP security and firewall facilities in conjunction with the Network iQ™ ENCO security architecture.

As more and more organisations make use of the services provided by the Internet, business solutions running over the Internet are set to become very common and cost effective. In addition to the general services currently offered by the Internet it is becoming apparent to many, that the Internet can be used to provide a very cost effective means of LAN interconnection. However the security considerations of allowing an organisation's sensitive information to travel across the Internet has, until now, prevented large scale use of the Internet for this purpose. This is because the Internet user has no control over where their information will be routed, or through whose hands it will pass. Since on it's journey through the Internet data can pass through many different organisations—ranging from commercial operations to research groups—the user has little confidence of the confidentiality and security of their data in transit. All of these issues can be solved by using the Network iQ™ router TCP/IP encryption facilities to allow secure VPNs to be created over the Internet and, at the same time, utilising the integrated router firewall features to maintain a tight control over normal Internet access.

The Network iQ™ ENCO Engine—High Performance with High Security

The Network iQ™ TCP/IP security architecture makes use of the ENCO (encryption/compression) engine to provide high performance, high security data processing. The ENCO is a plug in card with its own high performance CPU and dedicated DES encryption and LZS data compression hardware. Network iQ™ ENCO cards can be fitted to all models in the Network iQ™ range of routers, can service up to 90 links and support concurrent compression. The engine architecture is a veteran of the data compression arena and enjoys a strong and broadly representative installed base throughout Asia and Europe with users ranging from smaller business operations to large government and financial organisations.

Standards Based Architecture—All the way!

International standards are used to provide the router IP security architecture, including the following RFCs:

- 1825—Security Architecture for the Internet Protocol
- 1826—IP Authentication Header
- 1827—Encapsulating Security Payload (ESP)
- 1828—AH MD5
- 1829—ESP DES

In addition Allied Telesyn is committed to standards development through Internet Drafts such as those circulated by the IP Sec (IP Security) Commission.

Note: Interoperability with other vendors equipment is included as standard on Network iQ™ routers for situations where encryption is either not required or not

practical. For example when connecting to equipment with poor standards implementation.

Constructing secure VPNs using Allied Telesyn Products

The fundamental purpose of TCP/IP encryption is to allow the formation of secure VPNs over the Internet, where routers that are part of the virtual network can communicate freely but other Internet devices are under strict access control. This is possible because only routers on the Internet sharing a common set of encryption keys can communicate. Packets from other routers will be corrupted on decrypting and thus will be discarded and encrypted packets unable to be decoded unless the router possesses the key. Figure 2 shows how the LANs of organisations A and B are physically connected to the Internet (left), and how this translates into separate virtual networks (right).

Setting up Security Associations using single or multiple Encryption Keys

To create a virtual private network requires each router in the network to have a Security Association specifying, for each direction of data transfer, the encryption key and algorithm to use and the destination IP addresses to encrypt. A private network can be built using common Security Association information on each router (and therefore a single key for all routers) so that any of the routers can communicate with any other. Alternatively a more complex structure can be built by using multiple Security Associations (and therefore multiple keys) to control which routers can communicate. Each pair of inward and outward bound Security Associations requires one encryption channel, with the maximum number of channels supported being dependant on the ENCO model.

Figure 3: Constructing VPNs over Internet links.

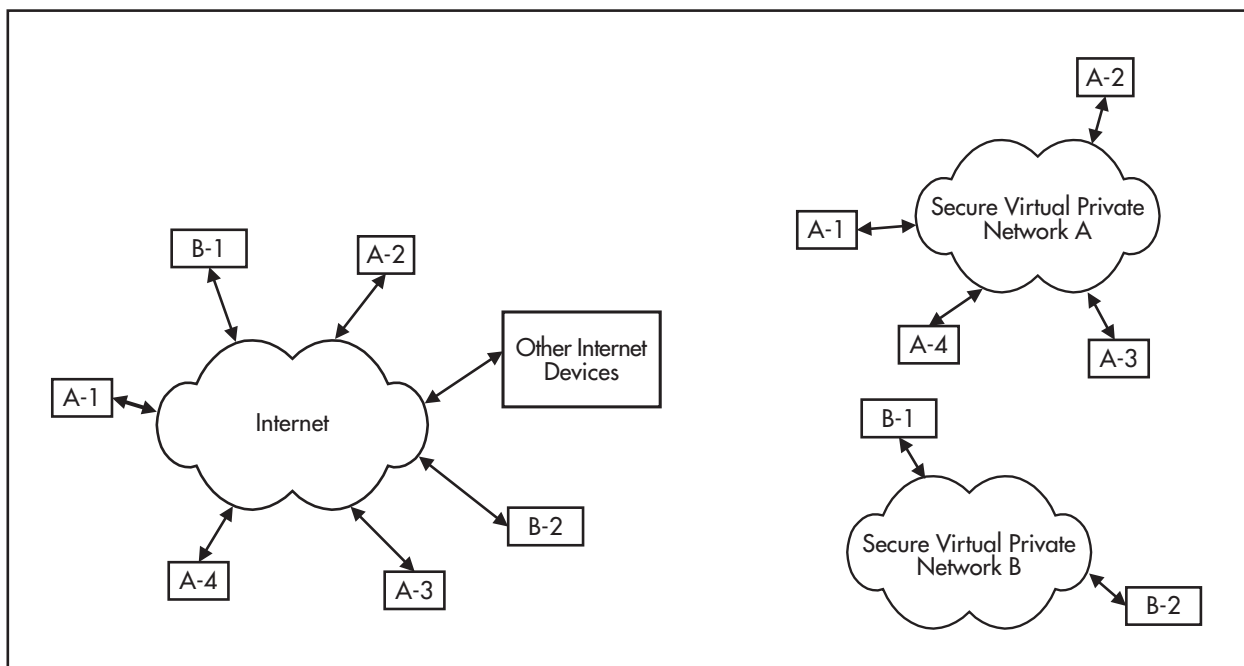
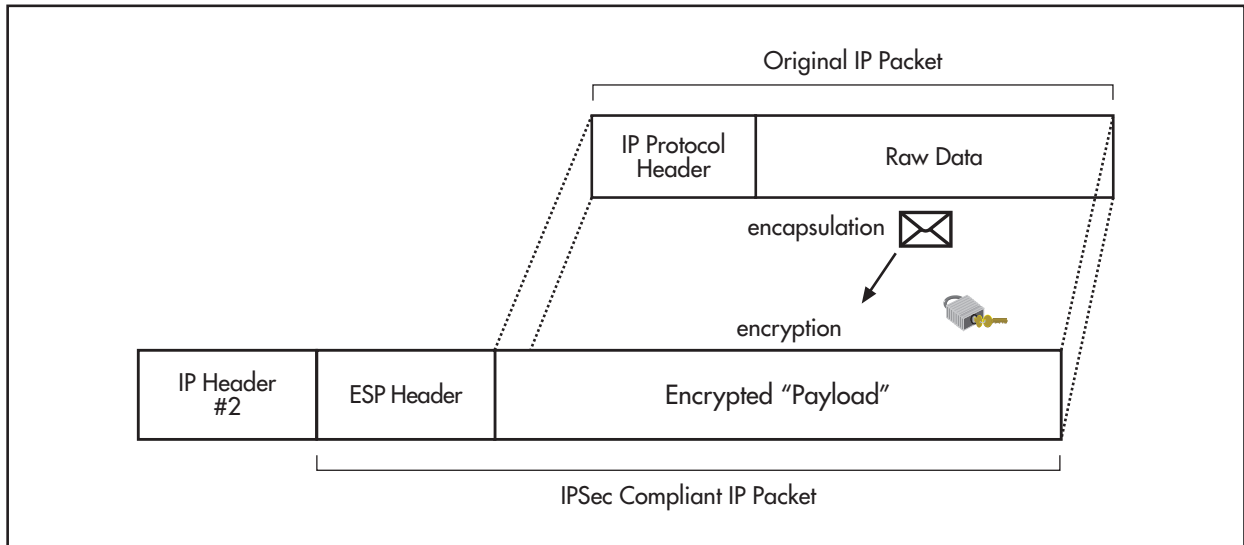


Figure 4: Encrypted IP Packet Architecture.



The Encapsulation Security Payload (ESP)

In operation the destination addresses of packets received from the LAN are checked against the addresses in each Security Association. If a match is made the packet is encrypted using the configured key and a Security Parameters Index (SPI) is included in the header to form an Encapsulation Security Payload (ESP). An un-encoded IP header is then placed in front of the ESP, so that the packet can be routed through the Internet. Having then travelled across the Internet, the packet arrives at the remote router and the SPI is used to locate the correct security association, and therefore key, to use for decryption.

During the creation of security associations the router assigns a random value to the SPI. This means that there is only a very small chance (one in 10 million) of invalid SPI values from an unwanted source causing the router to waste time on packet decryption.

If an SPI does match, but the Security Associations do not (for example if an attacker obtains knowledge of valid SPI values, but does not have the key) then the packet will be corrupted on decryption. This corruption can be picked up during decompression (if it is being used), or by the higher layer checksum, and will result in the packet being discarded.

Note: Used on its own ESP provides data confidentiality. For applications requiring higher security the packet authentication feature may also be used to provide both data confidentiality and authentication.

The DES Algorithm

ESP makes use of the U.S. military Data Encryption Standard (DES) algorithm operating in Cipher Block Chaining (CBC) mode. CBC mode combines the output of each previous 64 bit block during the creation of the next one, creating an error extension between blocks. Given that a DES key is 56 bits long there are more than 70,000,000,000,000 different possible keys, and since the keys used for encryption and decryption must match exactly before the packet will be accepted this system is very secure against attack.

Random Number Generation—A “Key” Factor.

Of fundamental importance to the security of this system is the privacy of the keys. Firstly there must be an equal chance that any possible key value is used. If this is not the case then this effectively translates into a reduction in key length, since any attacker no longer has to try every key. As mentioned earlier implementing encryption within pure software systems is problematic in terms of this requirement because all software random number generators are deterministic and can only ever be pseudo random. To avoid this problem the router uses the hardware random number generator on the ENCO to create keys, providing a truly random and thus a more secure solution.

Secure Distribution of Keys

In addition to this keys must be distributed in a secure manner. Network iQ™ routers achieve this by providing a once only display of the key to the security manager, who can then store and distribute it using known security methods.

Secure Key Storage

Finally keys must be stored in a way that preserves them over power down and prevents them from being discovered. With the router encryption system all keys are stored in non-volatile memory on the ENCO itself. This means that the keys are only accessible from the Network iQ™ ENCO processor, and not by the router operating system, providing far more security than PC based encryption systems (where the keys are simply stored on a hard drive). In addition the ultra security (ENCO-US) version provides physical access security and has tamper detection circuitry which erases all keys if the router case is opened.

Authentication Header

The Authentication Header (AH) is another IP security feature which allows the contents of a received packet to be verified. This feature can be used on its own, or in conjunction with ESP, to provide confidence that a received packet has not been changed in transit—in particular that data has not been taken out, added or changed.

The AH feature operates by processing the entire packet in order to produce a long hash value which is dependant only on the packet contents. If any part of the packet is altered then the hash value will no longer match. The concept of a hash value is very similar to a check sum, except the hashing algorithm is chosen such that it is a one way function. This means that it is easy to obtain a hash of the data, but not computationally infeasible to create a packet with a specific hash value or to modify a packet in such a way that the hash value remains unchanged.

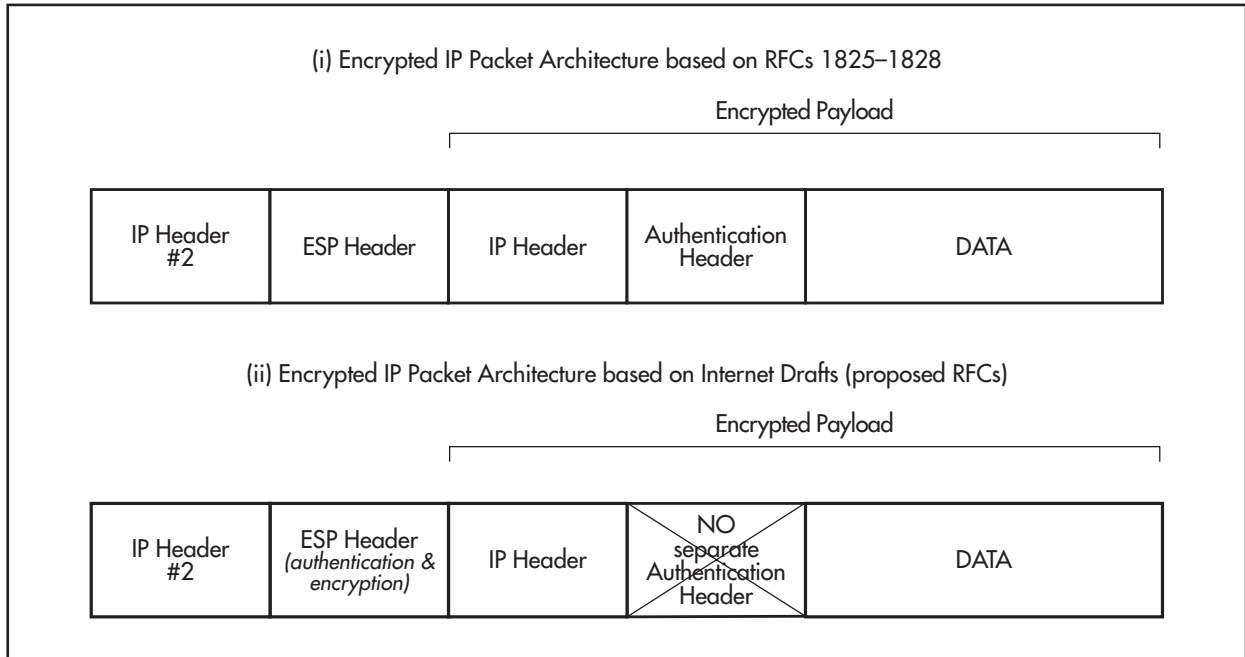
The operation of the AH is very similar to that of ESP, using the same concepts of Security Associations, SPIs, and keys. The difference is that the AH simply adds a header to the front of the unaltered data instead of encoding the data. Then at the receiving end the appropriate Security Association is selected, the key is obtained, and a new hash is made of the data. If the recalculated hash matches the one in the AH then the packet is unchanged.

A major limitation of the AH is that a large amount of processing power is required to perform the hashing—a laborious task if the AH process must be

carried out in software. The ESP encryption and compression processes carried out on the ENCO dedicated high speed hardware IC's provide a high throughput rate. By placing this task on the ENCO CPU the impact of this process on the router is minimised, however this still results in the reduction of throughput in the ENCO engine.

Figure 5: Changes in IP Encryption Architecture.

Allied Telesyn is committed to implementing industry standards, this includes changes both during and following the definition process. An example of this is seen in the above diagram which illustrates current proposed changes affecting AH header implementation.



MD5 Algorithm

A recognised one way function called MD5 is used in keyed mode as the AH hash function. Given that MD5 has a 128 bit key and result length, there are 3 x 10³⁸ different possible hash values—each of which is equally likely to be the result—making the AH a very secure authentication method.

Once again the keys are of fundamental importance to the security of this system. The router AH feature uses the same key creation, distribution and storage features as ESP to provide for a very high security level.

Additional Features—Controlling Internet Access

In addition to the secure VPN the router must also be able to provide controlled Internet access for non-organisation stations. The features to do this are already available in the router filter module. There are two main forms of access required:

- From an organisation to the Internet
- Into an organisation from the Internet

Both of these functions must be able to operate without compromising the security of the VPN, and must be able to provide for their own security requirements.

For access from the local network to the Internet it may be desirable to allow access to only selected Internet sites (for example to sites which have been vetted as being suitable), or to exclude access to specific sites (which are known to be unsuitable). In addition the source of an access also needs to be controllable, so that different rules can be applied to different users. Since the router firewall filtering can be selected by source address, destination address, and masks a complex set of access rules can be created to enforce any Internet access policy.

In the opposite direction the router firewall feature is used to allow outside parties access to specific parts of the organisations network, such as a web server, while preventing them from accessing sensitive network resources. This filtering is typically made on destination address and socket number, so that only the authorised services are available.

Further Security Enhancements using High Performance Compression.

Allied Telesyn products offer further advantages for corporate networkers through the ability of the Network iQ™ ENCO to provide high performance compression of data. In particular it offers an increase in throughput capability (dependent on the network characteristics) as well as further randomisation of data to offer even greater security.

Firstly, higher throughput is achieved by means of the STAC compression algorithm employed by the ENCO product. This compression is implemented in hardware. The STAC algorithm, can deliver compression rates of up to 11:1 (dependent on the nature of the data and of the network design as mentioned earlier) but latency can be particularly noticeable where this is implemented in software. In terms of throughput performance, however, users can expect to see double or better results in contrast to that of software compression implementations.

Secondly, greater security of data is achieved when compression is enabled as data leaving the compression process is no longer standard cleartext, rather it is in a form which requires a synchronised decompression process in order to be intelligible.

Thus the Network iQ™ ENCO compression facility, offers significant enhancements to an already impressive list of capabilities of the Allied Telesyn products.

Further Reading:

- White Paper on Security
- Virtual Private Networking Business Benefit Note
- GRE and Network iQ™ Router Application Notes
- Security and Firewalling Application Notes
- Product performance comparison notes

Other Features

Network iQ™ Routers offer a total solution for secure LAN internetworking and LAN access using both primary rate and basic rate ISDN, PSTN, frame relay, X.25 and leased lines. The Network iQ™ series of routers also supports channel aggregation using the PPP multilink protocol, bridging, data compression, bandwidth-on-demand, communications server and terminal/printer server capabilities, and many more features for cost-effective connectivity.