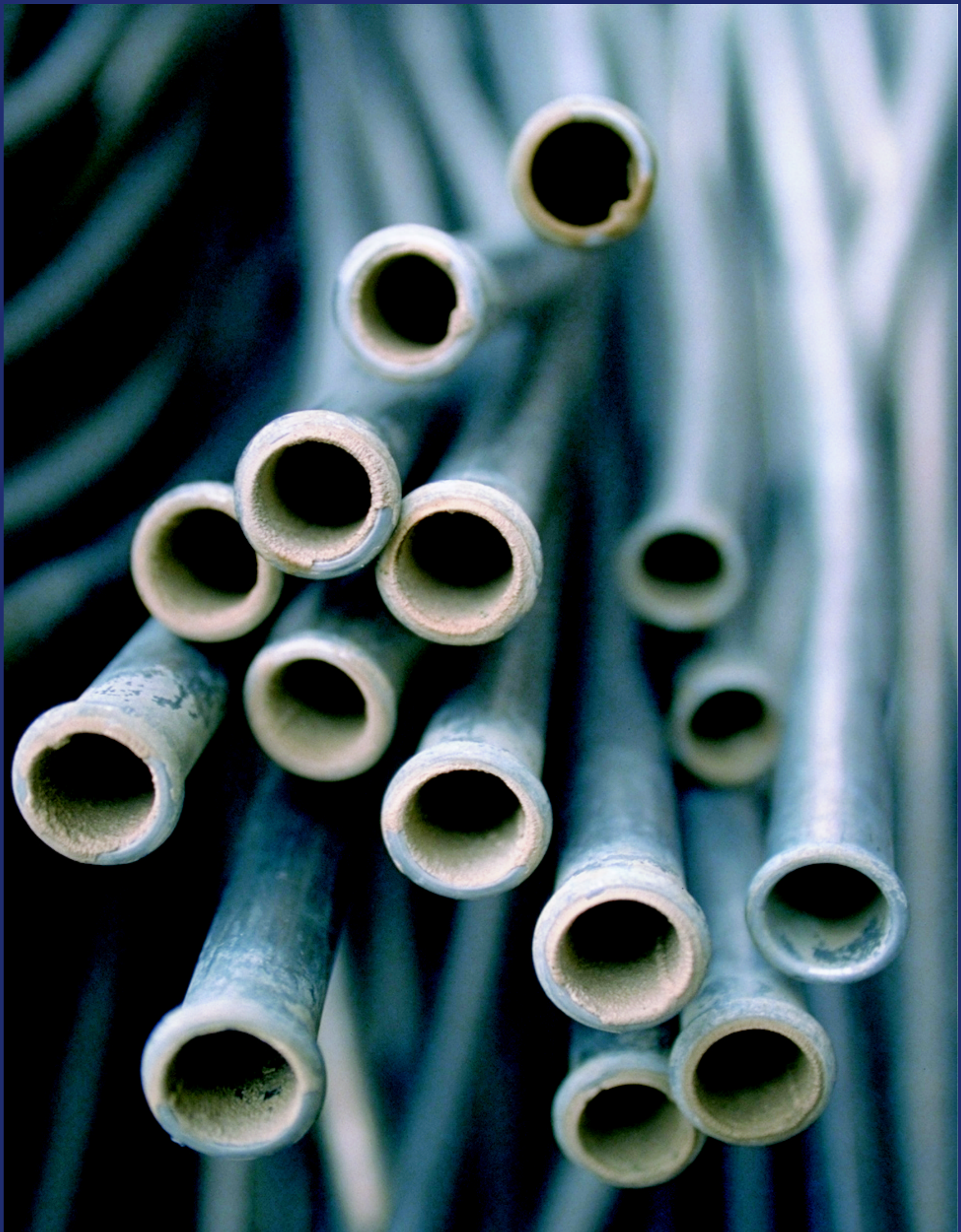
PRICEWATERHOUSECOOPERS

Alchemy

The Network Alchemy VPN Solution

A Technical Overview



Introduction

With the explosive growth of the Internet from 1994 to the present, a diverse array of information, and a wealth of connectivity resources have become available to millions of users. Many companies have come to rely on Internet connectivity as a basic part of their network services.

More and more organizations are trying to leverage their Internet connectivity and the widely available dial-up Internet access of national service providers to extend communications, increase exposure of their products, and enhance commerce. In the last few years the need to have virtually non-stop connectivity between employees, partners, vendors, banks, media, etc. has grown to the point that many organizations are looking to the nearly ubiquitous and cost effective connectivity available through the Internet. Typical corporate IT connectivity goals are:

- To enable the use of the Internet between corporate facilities to reduce, frequently massive, WAN charges and
- To enable the use of the Internet to provide mobile users a way of accessing corporate network assets, alleviating expensive long-distance charges.

Additionally, many companies that have Internet access realize that their customers, partners and vendors have access to this communication tool as well. With this in mind a third goal developed:

- To enable the use of the Internet as a communication medium between different corporate entities.

However, since the Internet is a public network, these goals must be met in such a way as to satisfy some basic security goals in order to be an effective tool for users:

- To ensure data confidentiality is maintained on the public network
- To ensure that the integrity of the data is intact
- To ensure both endpoints can determine the identity of the other endpoint by some strong means of authentication

It is the purpose of Virtual Private Network (VPN) technology to meet these six goals.

Since this need was first recognized, many approaches have been taken to meet the goals of the allusive VPN. Some have addressed only one or two of the connectivity goals. Some have fallen short on implementing the necessary services to meet the security goals. And finally, some have succeeded on both of these points but then failed to scale to meet the needs of large organizations. Network Alchemy's CryptoClusters™ not only provide an organization with the means of building a VPN capable of meeting these six goals, their high degree of scalability and unique manner of load sharing transparently between devices clearly differentiates them from other VPNs.

This white paper will focus on the VPN technologies that Network Alchemy's CryptoCluster™ VPN servers leverage and the unique and exciting, technology that clearly differentiates Network Alchemy's CryptoClusters™ for a company seeking to get the most out of its investment in Internet connectivity.

Technologies used in Network Alchemy VPN Solutions

Remote Access VPN technologies:

PPTP and L2TP

Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) are PPP tunneling protocols that were designed for remote access VPNs, and both were created to satisfy the second connectivity goal. PPTP is a Microsoft invented protocol that has been integrated into their Windows clients. L2TP is the IETF standards track protocol which came from the integration of Cisco's Layer 2 Forwarding (L2F) and PPTP. L2TP is eventually expected to replace PPTP. At the moment both protocols are in use, although they are typically deployed in different scenarios.

In both scenarios, a Network Alchemy CryptoCluster™ can be situated on the company's premises, typically near the Internet router. CryptoClusters™ work in conjunction with firewalls, providing access control, and may be placed in front of a firewall, behind a firewall or in parallel with a firewall in a variety of manners. Specific implementation strategies will be discussed in a future PricewaterhouseCoopers white paper.

A typical PPTP scenario, involves remote users dialing into an ISP account using a local dial- access number. The ISP is not involved in this protocol, however. Once a PPP or SLIP connection is established between the dial-in user and the ISP, a PPTP connection is established with a PPTP server on the user's home network. Essentially, a virtual PPP connection is established between the PPTP client and the PPTP server. The PPTP client software and the server renegotiate PPP parameters such as IP address, DNS server, and so on. Note that the client still uses the IP address originally negotiated with the ISP, for the outer packet header. This will be diagramed below.

In more detail, what happens is that once the original PPP or SLIP connection is established, the formation of the PPTP connection begins with the establishment of a TCP connection from the PPTP client to the PPTP server. This session will remain open for the duration of the PPTP connection. This TCP connection is the control connection for the PPTP tunnel, and it is used to communicate control information for the PPTP connection. The data packets originating in the PPTP client are encapsulated in PPP frame, minus any media specific headers, that is then optionally encrypted, encapsulated again using a modified GRE, Generic Routing Encapsulation, header. This is finally encapsulated in another PPP, or perhaps SLIP, frame and then forwarded to the ISP's NAS or router. The ISP's router strips off the outer frame encapsulation and routes the modified GRE packet across the Internet to the PPTP server. The PPTP server strips off the GRE encapsulation and decrypts the nested PPP frame if necessary. Finally, the PPTP server removes the PPP framing from the original datagram, and forwards the datagram onto the internal network (1).

Diagram 1 – A PPTP Data packet

Local PPP/SLIP	GRE header sa:1 da:2	Inner PPP header	IP packet sa:2 da:any	data

SA1: locally provided IP address

SA2: address provided by the PPTP server

DA2: PPTP server

Some firewalls will not pass GRE packets by default, and in cases where the VPN server is placed behind a firewall or filtering router, an access list entry needs to allow PPTP to pass to the PPTP server.

PPTP client software is available for free from Microsoft for Windows platforms, but Microsoft’s implementation of PPTP has had numerous security problems reported in the past. However, PPTP can be used in conjunction with IPSec to provide a higher level of security. This will be discussed in more detail in the following section on IPSec.

L2TP can be used in one of two ways. One is much like the mechanism used in PPTP the other involves a NAS to home gateway functionality that may be initiated at the dial-in POP. In the typical L2TP implementation, the ISP is involved in the protocol, meaning that the dial up ISP must support L2TP on their NAS, which the L2TP protocol specifications calls the L2TP Access Concentrator (LAC). In this deployment of L2TP, the client is not required to run any additional software other than that required to make the initial PPP connection with the ISP. The ISPs LAC participating in the L2TP protocol, or the authentication server, will recognize the user’s domain name as one that is participating in an L2TP VPN. The LAC establishes an L2TP connection with the L2TP Network Server (LNS) that resides on the user’s home network. The network protocol information, including client IP address, for this PPP connection, initiated from the client machine toward the local LAC, will actually be negotiated with the LNS. Once complete, it is as though the client has “dialed into” their corporate network even though no long distance call had to be made and no special processes on the client side were needed.

In more detail, the IPS’s LAC passes UDP packets containing the client’s PPP frames back and forth with the LNS. All of the PPP frames forwarded by the client to the ISP’s NAS are encapsulated within these UDP packets and routed across the Internet to the VPN server. The LNS strips off the UDP encapsulation, removes the PPP framing, and forwards the resulting packets onto the corporate network (2). See Diagram 2.

Diagram 2.

Local PPP/SLIP	GRE header sa:1 da:2	Inner PPP header	IP packet sa:2 da:any	data

L2TP does not have a specific encryption protocol. However, it is possible to use one of the PPP encryption options or IPSec to secure L2TP. This is discussed in the section on IPSec.

PPTP and L2TP are very similar protocols in terms of functionality, and it is possible to use L2TP in scenarios like that shown described in the PPTP overview above.

A disadvantage of using these protocols in a VPN, besides the level of security often afforded, is that PPP is a link layer, connection oriented protocol. In some cases it is not ideal to add this extra layer of connection protocol to a connectionless infrastructure like the Internet.

IPSec and IKE Technologies

IPSec is a set of standards that specify an open architecture for the inclusion of a wide range of security mechanisms to provide data authenticity, confidentiality, integrity and non-repudiation services for the IP network protocol. IPSec has no allegiance with any particular method of encryption or authenticity verification, so corporations may choose from a wide range of algorithms to suit their particular security requirements. As older encryption algorithms become outdated and are replaced, new encryption algorithms may be used with no changes to the IPSec protocol. In addition, IPSec allows for the use of different methods for key exchange. The standards are written so that new key exchange protocols, authentication procedures and encryption algorithms can be integrated into IPSec in a way that will ensure interoperability with other organizations using IPSec compliant equipment that support the same protocols
and algorithms (3).

IPSec was not created with only the final goals of VPNs in mind, but with the intention of providing security services for any type of IP connectivity that might need these services at the network layer. However, the IPSec authors were well aware of the needs of VPN technology, and their specifications have met many of these goals in an extremely flexible and extensible way.

Among the security mechanisms that can be used with IPSec presently, confidentiality can be provided with Triple DES encryption (Triple DES), using a 168-bit key space. This is presently one of the strongest encryption mechanisms commercially available and is secure enough that it is used even in large financial transactions taking place across untrusted networks such as the Internet. Triple DES was derived from DES, which uses a 56-bit key. DES is now essentially insecure, since devices have been constructed which are capable of breaking DES encryption by a brute-force search over the key space in a matter of hours. DES should not be used for any application requiring a very high level of confidentiality. Triple DES, on the other hand, should remain secure for some time to come. Triple DES, however, is computationally extremely demanding, and even many hardware implementations have difficulty "doing the math" involved in encrypting or decrypting substantial quantities of Triple DES data. For these reasons, when comparing VPN products that claim Triple DES encryption as a mechanism for providing confidentiality, it is very important to make sure that performance data are given using Triple DES. Any performance numbers given with DES should be disregarded as Triple DES requires at approximately 2.5 times slower than DES at best (4). Network Alchemy's CryptoCluster™ products support DES, Triple DES, Blowfish, IDEA, RC5, and CAST-128 for encryption within IPSec, as well as HMAC-SHA-1, HMAC-MD5 and HMAC-RIPE-160 for authentication
within IPSec.

Triple DES, as well as the rest of the encryption ciphers just mentioned, is a symmetric key cipher. This means both parties involved in an encrypted communication process must share the same key. The confidentiality of the communication depends completely on the secrecy of this key. In order for both sides to reach an agreement on the key to be used, it is necessary for the peers to use a key exchange protocol. Network Alchemy's CryptoCluster™ VPN server uses IKE, the Internet Key Exchange, for automatic key exchanges. IKE is an IETF proposed standard required to be supported by any IPSec compliant device, and it is documented in RFC 2406. IKE is a protocol that supports automatic, authenticated key exchange, and that may be used with or without IPSec compliant X.509v3 certificates. Network Alchemy CryptoClusters™ have an integrated CA that may be used for the generation of such certificates if their use is desired. Verisign OnSite is also supported in the initial release of CryptoClusters™. In future releases, support is planned for the Cisco Enrollment Protocol (CEP), as well as Verisign and Entrust format certificates. If certificates are not used, shared secrets can be used to authenticate the key exchange. Besides support for IKE, keys can be statically configured although this is not recommended (5), (6), (7).

Design Solutions

The IPSec protocol is flexible enough that it can be used to attain all of the connectivity goals required of a VPN while providing strong confidentiality and authenticity services. The following paragraphs will examine each of the basic connectivity scenarios and see how a Network Alchemy CryptoCluster™ can use IPSec to provide the required connectivity in a secure fashion. Specific implementation strategies will be discussed in an upcoming PricewaterhouseCoopers white paper.

LAN to LAN: inter- or intra-corporation

To meet the goal of secure LAN-to-LAN connectivity across the Internet, a CryptoCluster™ sits at the edge of each network. The VPN servers are configured to establish communication with one another and, using IKE, establish an ISAKMP security association (SA). The ISAKMP SA remains in effect for a period negotiated during its formation, and it is used to establish SAs for use by the devices each of the CryptoClusters™ protect. In some situations, only one other SA will be established and that SA will carry the information such as encryption type, digital signature protocol, and keys that the devices will use to protect the traffic behind each of the CryptoClusters™. Alternatively, different SAs may be established for each flow or with some intermediate range of granularity as required by the existing security policy. The granularity is specified by the configured policy of the CryptoCluster™. After the lifetime of an SA has expired, a new security association will be formed in order to continue secure communication. This requires re-keying. Either time or number of bytes encrypted defines the lifetime of an SA. As a result of re-keying, different session keys will be used for different parts of a particular flow, to help defend against cryptanalysis.

The machines protected on each LAN in this fashion require no additional software or configuration of any kind. The CryptoClusters™ act on their behalf as IPSec gateways to provide the necessary security services mandated by the corporate security policy.

The tunnel mode of operation, which is used whenever IPSec gateways are used to protect traffic, protects the original source and destination IP addresses as well as the data contained in the original packet. This protection allows private IP addresses to be used on the protected LAN segments, such as the 10.0.0.0 network as discussed in RFC 1918. The traffic with private addresses can be passed over the Internet since the IPSec header that encapsulates it will hide the original IP header containing the private IP addresses. The tunnel mode of IPSec operation also prevents detailed traffic analysis from being performed on the traffic passing between the two LANs. (3)

Remote access using IPSec

For remote users, IPSec may be used as an alternative to or in conjunction with PPTP and L2TP, and we will first discuss using IPSec exclusively.

In an IPSec only solution, the client must either have an IPSec capable TCP/IP protocol stack or run an additional piece of software to implement IPSec on their client node. Since Windows platforms do not currently have IPSec capable TCP/IP protocol stacks, Network Alchemy provides, free of charge, client software that is implemented as an NDIS Intermediate Device Driver. This software, called the CryptoStation™, sits between the TCP/IP protocol stack and an NDIS NIC driver or the NDIS WAN wrapper used for PPP connections. This is commonly referred to as a 'bump in the stack' implementation. After a datagram is prepared for delivery by the TCP/IP protocol stack, the CryptoStation™ intercepts the datagram and compares the datagram against the configured policy of the CryptoStation™. If the policy requires protection services for the datagram, they are applied to the datagram. The final datagram is then passed through the NDIS interface for delivery.

Client Configuration for IPSec security

Regardless of whether the TCP/IP protocol stack is IPSec capable or the CryptoStation™ is being used, IPSec must be configured with detailed security policies so that the client machine will understand which security services need to be provided for which datagrams. The process of policy establishment and configuration is one of the most daunting portions of any VPN implementation, but is absolutely critical if the proper protection services are to be applied. Network Alchemy uses a management station to manage the policy and configuration not only of all the Network Alchemy CryptoClusters™, but also of the CryptoStations™ provided to the remote users. The management station software is implemented as a fully compiled Java application, the Network Alchemy CryptoConsole™, which is discussed in more detail later.

Besides being useful in dial-up scenarios, the CryptoStation™ is also of use if a few machines in remote locations having dedicated Internet connectivity need to establish secure connections back to the resources at a corporate headquarters.

When used for dial-up connectivity, the user establishes a PPP connection with an ISP. As in the PPTP scenario discussed above, the ISP is not involved. However, unlike the PPTP scenario, that is all the user has to do. The CryptoStation™ handles the establishment of SAs and the provision of protection services according to its configured policy based on the protocols used, the destination address and other selector information in the datagrams prepared by the TCP/IP protocol stack. The user does not play any part in this process, and does not need to be aware that security services are being provided. For strong authentication, IPSec can use IPSec compatible X.509v3 certificates. During SA establishment, the CryptoStation™ retrieves the certificate using the CryptoAPI, and the certificate is retrieved from the appropriate Cryptographic Service Provider. In order for a user to utilize a certificate that is stored in the client machine, the user is required to provide a password in order to ensure his identity.

IPSec with L2TP or PPTP

IPSec used in conjunction with PPTP or L2TP provides greatly enhanced security especially with an encryption algorithm such as Triple DES. In such a configuration, the remote client would dial the ISP as before, and start a PPTP session with the PPTP server as usual. However, this time the CryptoStation™ or IPSec compatible TCP/IP stack establishes SAs with the IPSec server to protect the traffic to and from the PPTP server according to its configured policy. After the SAs are established, the communications with the PPTP server proceed as normal, and all the communication with the PPTP server will be protected by IPSec.

Similarly, in the typical L2TP scenario, IPSec can be used to protect the L2TP traffic between the ISP and the customer location. The ISPs access servers can be configured to establish SAs with an IPSec gateway that may or not coincide with the L2TP endpoint inside the company. It should be noted that the IPSec protection does not extend all the way to the client unless the IPSec with L2TP or PPTP has been initiated at the client station. This could mean that the traffic from the client to the ISP is not protected.

IPSec may be used in a situation similar to the usual L2TP scenario, replacing L2TP entirely. Security cautions apply even more strongly in this scenario as the traffic between the client and the ISP is now passed completely in the clear unless some PPP encryption is being used.

Regardless of the strategy chosen for a dial-up VPN implementation, Network Alchemy CryptoClusters™ have an integrated RADIUS client This ensures that a company that has already made an investment in remote access to the level of implementing such authentication servers can protect their investment. Additionally, this provides the product with greater scalability and integration with the existing network infrastructure.

For extranet connectivity, the most important features of IPSec are its capacity to provide strong security services and its status as an IETF standard. There are numerous IPSec products that are guaranteed to interoperate to the extent that they conform to the standards.

Clustering: Scalability and Reliability

Background

Clustering is the use of multiple machines providing the same service and behaving as a single, virtual machine with the ability to provide workload distribution between member machines and high availability in the event of the failure of one or more member machines. The promise of clustering is the ability to provide scalability and fault tolerance. Present clustering implementations have primarily provided multiprocessor, shared disk types of load sharing and fault tolerance. For example, Microsoft now has a clustering scheme that allows two servers to provide fail-over capability for one another. If one machine is an FTP server and this machine fails, the other machine can assume the IP address of the failed machine and start the services required for FTP serving. However, a client downloading a file via FTP during this fail-over process will have their FTP session terminated. The cluster member to which FTP serving has failed-over is aware that the other cluster member has failed, but does not have knowledge of the status of the interrupted file transfer and, more fundamentally, of the underlying TCP connection of the client to the original FTP server. The client is forced to reestablish the connection and begin the file transfer again. However, what Network Alchemy, Inc. has developed and patented is a way to cluster at the IP packet processing level. Packet flows are divided up into workloads that are off-loaded to the various nodes as their processing power allows. The state of each of these flows is then shared across the cluster and fail-over of any flow becomes possible.

Network Alchemy's DaveOS

Network Alchemy's CryptoCluster™ is architected around a small, about 1.4 Megabytes, proprietary operating system called DaveOS. DaveOS was not designed with VPNs or any other particular application in mind. Rather, DaveOS was created to solve the fundamental problems of network packet processing, load-sharing, fail-over and scalability. The Network Alchemy CryptoCluster™ VPN server is the first application of this solution, and the code required to perform the VPN activities discussed above run as applications on the DaveOS clustering kernel.

In the following sections, we discuss how DaveOS solves the fundamental problems of clustering, and how the power of DaveOS' clustering capabilities are harnessed by the Network Alchemy CryptoCluster™ VPN server to provide a level of reliability and scalability that make the Network Alchemy CryptoCluster™ suitable for even large enterprises or service providers.

In the configurations we have discussed so far, the Network Alchemy CryptoCluster™ VPN server may be configured either as a single, dual-homed routing device or a cluster of such devices. Although a single-homed configuration is possible, it is not discussed here. In all cases, the Network Alchemy CryptoCluster™ VPN servers need not be implemented as single device. Rather, it can be composed of a number of Network Alchemy CryptoCluster™ nodes organized as a cluster. In such configurations, each Network Alchemy CryptoCluster™ node has a unicast IP address on each of its interfaces appropriate for the subnet to which they are attached. Additionally, all of the outside interfaces share a distinct unicast IP address appropriate for the subnet of the outside interfaces. Likewise, the inside interfaces share a distinct unicast IP address appropriate for the subnet of the inside interfaces. These shared IP addresses are used for communication with and through the cluster.

We will now take a brief look at what happens when Network Alchemy CryptoCluster™ nodes configured in such a cluster are first installed into the network. First the devices establish communications with each other. Identity is established through strong authentication, and subsequent communication between the devices is strongly encrypted and propagated on the inside interfaces. One of the devices is elected the master of the cluster. The role of the master is detailed in subsequent paragraphs.

When the CryptoStation™, or any remote client, attempts to establish an SA with the cluster for the purpose of protecting traffic to and from the internal network, it is the shared outside cluster IP address with which the CryptoStation™ or client is configured to use as the IPSec gateway for traffic. When the client request arrives at the cluster, it is processed by the member of the cluster who owns that workload. The master decides which cluster member will be responsible for processing which workload, and therefore, which node will process the client's traffic and establish the SA. This member proceeds to establish the SA with the client. All the traffic seen by the client from the cluster is source addressed with the shared outside cluster IP address as the CryptoStation™ or remote client expects. Once the SA is established, the cluster member informs the other members of the cluster of the details of the SA formed, i.e., encryption and integrity algorithms, associated keying material, etc., using the encrypted communication channel on the inside interfaces.

Cluster modes of operation

For each packet that arrives addressed to the cluster, there are three different distribution techniques by which the cluster ensures that the packet is delivered to the appropriate node for processing. These are known as forwarding mode, unicast mode and multicast mode. In forwarding mode, the master answers the ARP requests for the MAC address of the virtual, shared cluster IP, address with its own MAC address, and all packets are initially delivered to the master for subsequent distribution. It is then the master's job to forward the packet to the correct member of the cluster for processing. Alternately, in unicast mode, the cluster members share a virtual MAC address from the addresses assigned to Network Alchemy by the IEEE. In this way, they all accept each packet and decide, based on what workloads they have been assigned by the master, whether the processing of a given packet is their responsibility. Although this may seem ideal, some switches will not accept that a single MAC address should be forwarded to multiple switch ports. Multicast mode was designed as one solution to this problem. In mulitcast mode, all the devices which need to forward packets to the cluster are configured to use a multicast MAC address, when forwarding packets to the shared IP addresses of the cluster.

This entire communication infrastructure is used by the Network Alchemy CryptoCluster™ to provide the network redundancy and scalability advantages elaborated in the following sections.

Workload Balancing

After the cluster elects the master, the master queries each cluster member to assess performance parameters in order to determine how much of a workload each cluster member is capable of processing. The master assigns each flow to one of 1024 "work buckets" based on a hash of various parameters sometimes including the source and destination IP addresses. Each of these "work buckets" is assigned to a cluster member. The master continually assesses the load on each of the cluster members, and performs calculations to decide whether redistributing the "work buckets" among the cluster members would be advantageous. If the master determines that a performance improvement could be obtained through such redistribution, it notifies the cluster members of their new workload assignments. This is done gradually in one bucket increments. Because of the fact that all of the cluster members keep knowledge not only of the SAs, but also detailed knowledge of the state of TCP connections, including sequence and acknowledgment numbers and window sizes, the transition of workload between cluster members is seamless and transparent.

Scalability

The nature of the workload balancing scheme discussed above is such that an enterprise may start with a relatively small, single Network Alchemy CryptoCluster™ without being concerned that their needs may eventually outgrow it, rendering it obsolete. When an organization reaches the point that the current server capacity is in danger of being reached, another, or even multiple, Network Alchemy CryptoClusters™ nodes may added and the devices easily configured to work together in a cluster. If a CryptoCluster™ node is of equal capacity to another, the workload will be evenly split between them, but even if the second device has a much higher capacity than the first, the first will still be used in accordance to its performance ratio with the second, and more powerful, device.

Active Session Fail-over™

As discussed above, the ability of current clustering technologies to gracefully handle the failure of a member device, whether due to actual failure or administrative downing, is typically poor. With DaveOS, this situation is greatly changed. Due to the manner in which the cluster is constantly kept apprised of the state of the TCP connections, as well as the SAs in the VPN implementation, the failure of a member is detected by the cluster members and that member's workload is reassigned to other members. This entire series of events typically occurs in 250 milliseconds. Even if the master itself fails, this failure is detected by the other cluster members, which promptly elect a new master who then redistributes workload information to the other members. This additional overhead results in a transition time of around 500 milliseconds.

It is this fundamental ability of DaveOS to provide Active Session Fail-over™ that sets it apart from other clustering solutions. This ability is fundamental in a truly scalable VPN implementation for the following reasons. First, dropping an IPSec connection means that all of the TCP/IP connections using that IPSec connection are also terminated. The remote client machine, for example, is forced to renegotiate an SA with a gateway device. These SA negotiations require computationally expensive, and time consuming, modular exponentiations. Even after the SAs are renegotiated, the sessions that were active at the time of failure must be re-established. For a VPN implementation supporting a large number of SAs and sessions, a substantial amount of time could pass before the state of communication that existed prior to the failure could be re-established.

These are precisely the problems that DaveOS eliminates, and the Network Alchemy CryptoCluster™ is merely the first application to leverage this new level of IP clustering technology. Together DaveOS and the VPN technologies integrated into the Network Alchemy CryptoCluster™ VPN server give an organization the tools to meet the goals of many VPN projects with a truly remarkable degree of both scalability and reliability.

Manageability: The Network Alchemy CryptoConsole Java Management Station

The issues related to securing network communications are complex. Just deciding on a corporate security policy is difficult enough. Configuring and enforcing this policy can be quite challenging for a network administrator. Since Virtual Private Networks (VPNs) are a very important piece of a security strategy, configuration and management of the associated policies are key in maintaining corporate security. Also, since VPN hardware is by nature dispersed, the management of a VPN can be especially cumbersome. It is very important that the configuration be as easy as possible to ensure that it is done properly and effectively. Complexity invites error, yet the policies that the VPN configuration must hold are quite intricate. In order to feel confident that the proper degree of security is applied to sensitive corporate data, a management solution that allows administrators to easily configure and validate policy as well as view the status of VPN tunnels, endpoint devices and

active users is an absolute necessity.
Rather than management being an add-on to the Alchemy solution, the CryptoConsole™ is the heart of the system and acts as the overseer of the entire VPN architecture. All of the elements in the Alchemy VPN architecture are easily and visually managed via the CryptoConsole™. The CryptoConsole™ is able to perform configuration, monitoring, and diagnosis of all tunnels in the CryptoCluster™. This truly easy-to-use and comprehensive management tool runs on a software platform of Windows95, Windows NT, or Solaris SPARCstation. It is a full Java application allowing for GUI based generation and examination of security and /or layer-2 tunnel policy and activity. As a result of the CryptoCluster™ being managed as a single device, no matter how many nodes comprise the cluster, configuration and maintenance overhead is greatly reduced. The CryptoConsole™ keeps track of the latest policies configured by the network or security administrator. Should any node in a cluster discover its version of the configuration is older, it will automatically and securely update its configuration file with no user intervention. This ensures that all elements in the CryptoCluster™ are in sync and their configurations up to date.

The Console handles all of the VPN set-up. It is the one place administrators go to add new devices or users of all types to a VPN. In order to add new Crypto nodes into a cluster or to create a completely new cluster the administrator simply runs the “Install Gateway” wizard from the management station. The CryptoConsole™ will inform the administrator of a very short list of information that needs to be typed into the serial console of this new cluster node. For security purposes, this information will include an eight-hour security token for access into the cluster. This is all the console configuration ever needed on any node. This gives administrators the option of staging the new hardware at a central location by entering this required security information into the new node before deployment. At this point, installation can be done by any personnel without worry as to potential security compromise. Less experienced employees can be used to physically plug nodes into the network. The remainder of the required configuration information will be given to the new cluster node from either another cluster member or from the CryptoConsole™ directly. Since the configuration is centrally created, managed, monitored and changed, all elements work together seamlessly. Built-in policy testing ensures that logical and correct security policies are in place.

Remote Client: CryptoStation™

The CryptoStation™ is capable of differentiating traffic based on very granular criteria. Filters can be defined to identify source and destination IP address, IP protocol number as well as source and destination TCP or UDP port numbers. This policy is installed as part of the overall client software. The user never needs to be concerned with configuring the policy on their PC. This is something generally out of the realm of expertise of the user. Also, this is generally a corporate security policy issue best handled by the network administrator. The policy is configured on the CryptoConsole™ management station. Certificates are generated for the user with the aid of the CryptoConsole™. These certificates will identify the user absolutely. The CryptoStation™_ is then given to the PC user via a file available for transfer via a disk or email. This file containing the CryptoStation™, X.509v3 certificate and policy is encrypted by the CryptoConsole™ using Triple DES and must be decrypted on the client PC, using the user’s password. Since the policy is configured on the CryptoConsole™ the administrator is able to define and configure policy both on the gateway CryptoCluster™ itself and the client side to ensure that it is correct and consistent. Configuration by the management station allows for the generation and examination of tunnel policy for the CryptoClusters™ and the CryptoStation™ prior to installation.

The user simply installs the client CryptoStation™ using Installshield. In order to ensure the identity of the user, not just the device, the user must supply the CryptoStation™ with a specified password before being able to utilize the IPSec encryption or authentication capabilities. A password must also be supplied to the client periodically to ensure that the PC has not left the user's control. There is a systray application that enables the viewing of CryptoStation™ status to ensure it is working in order to aid in any troubleshooting that might be necessary. The next release of the CryptoStation™ will enable the automated updating of policy without user intervention to further ease in the management of user devices once installed on client PCs.

The CryptoStation™ is the first commercial IPSec client implementation not bound to one gateway and interoperable with any standards compliant IPSec implementation. This client is actually a completely standard IP stack running under the Windows stack with full support for IPSec. The CryptoStation™ has the ability to negotiate security associations with many different devices and talk to them all simultaneously. It has the ability to communicate with any entity performing IPSec with varying policies for each destination as well as to concurrently communicate in cleartext with other endpoints.

Conclusion

Network Alchemy's solution has addressed each of the six goals for VPNs through its use of standards based encryption and communication protocols. The Network Alchemy CryptoCluster™ VPN provides a solution that uses the Internet, allows mobile users access, connects to non-Network Alchemy products that are IPSec, L2TP or PPTP compliant, and provides capability to ensure confidentiality, integrity, and strong authentication using public key cryptography. Moreover, Network Alchemy has leveraged the clustering power of DaveOS with dynamic workload balancing and Active Session Fail-over™, to provide a solution with a high degree of scalability and reliability while providing a single point of management for all CryptoClusters™ and CryptoStations™ in the enterprise.

The opportunities to use this technology provide a wide variety of implementations that can be used for large or small corporations.

About the Author:

Jason Dowd is a Senior Associate in the Technology Risk Services practice at PricewaterhouseCoopers, based in St. Louis, MO. Jason has more than five years of experience working with IP networking, Internet, and Electronic Commerce solutions. Jason can be contacted at jason.dowd@us.pwcglobal.com.

References:

(1) K. Hamzeh, G. S. Pall, W. Verthein, J. Taarud, W. A. Little, G. Zorn, " Point-to-Point Tunneling Protocol (PPTP)", draft-ietf-pppext-pptp-07.txt

(2) A. Valencia, K. Hamzeh, A. Rubens, T. Kolar, M. Littlewood, W. M. Townsley, J. Taarud, G. S. Pall, B. Palter, W. Verthein, "Layer Two Tunneling Protocol "L2TP"", internet-drafts/draft-ietf-pppext-l2tp-12.txt

(3) S. Kent, and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

(4) N. Doraswamy, P. Metzger, W. A. Simpson, "The ESP Triple DES Transform", draft-ietf-ipsec-ciph-des3-00.txt

(5) D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

(6) D. Harkins, and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.13 Pre-Examination Report to the Audit Committee of the Board of DirectorsPre-Examination Report to the Audit Committee of the Board of Directors

(7) D. Piper, "The Internet IP Security Domain Of Interpretation for ISAKMP", RFC 2407, November 1998.

Your worlds

Our people