Encryption Key Management in Large Scale Network Deployments

by
Franjo Majstor & Guy Vancollie

1. Introduction

All corporations need to protect their business transactions, customer data and intellectual property. At a minimum, data loss or compromise can create public relations nightmares and even seriously hurt market reputation. In the long run, they can impact customer relationships or create serious financial damage from fraud, information theft or public disclosure of intellectual properties. This problem has presented IT with a technological challenge because the ideal network data protection solution should require no change to network infrastructure, should not impact network performance, must work over any network topology and must secure any type of traffic. The challenge facing information security professionals is to secure data in motion as it has never been possible before. It is obvious that encryption is the solution to address confidentiality and integrity of the data while it transits lines that we have no control over, however its limitations have hampered its deployment specially on large scale networks. Standards are normally there where interoperability amongst different vendor solutions should take place and multiple good ones have done that, like, for example, the IP Security (IPSec) standard framework. Although IPSec delivered a portion of the solution, it also introduced its own limitations and unnecessary overlay to an existing network infrastructure making it even more difficult to manage, maintain and operate.

2.*Large Scale Network Issues*

2.1. Performance

Not so long ago it used to be that data network infrastructures were used only for the bulk transfer of data over slow links of various, mostly unreliable quality. The data carried over those network infrastructure was less important, and even if stolen, modified or lost, there were always multiple paper copies and forms in existence to replace the incorrect data when needed. Nowadays a modern high speed network infrastructure carries the most crucial pieces of information as well as multiple crucial applications that companies depend upon for their existence. Adding encryption to the communication paths, unless assisted with specialized hardware, typically slows down the overall communication speed and, therefore, impacts the usability of the high speed communication paths.

2.2. Redundancy

High speed, high performance networks are required to stay up all the time, no matter what happens with individual communication components. Therefore, modern network design includes multiple redundant devices as well as multiple available paths built into the network itself. Redundancy built into the network keeps the availability of the communication paths between multiple points in the network, however it often causes difficulty for security mechanisms.

2.3. Load Balancing

Multiple redundant paths do not necessarily have to work in a master slave or active-standby mode, but could be active and used simultaneously to do load balancing and share the traffic load across the multiple links. This is the preferred way for efficient networks to use multiple available links, but also has unfortunately some security implications. Security relationships are typically fixed between peers and are in trouble when they lose peer relationships that have to be dynamically established when network traffic chooses another path to the same destination.

2.4. Multicast

Any kind of group communication, and multicast is just one of them - requires group security member relationships as well as group member control if any of the communication peers leaves or joins the group. That makes the encrypted group communication extremely difficult with a heavy overlay of the peer to peer relationships that grows exponentially with the number of peers communicating. It is a known mathematical fact that for “n” number of peers it is required to have “n*(n-1)” peer to peer relationships and that times two if each direction has to be secured separately.

2.5. MPLS

Multi Protocol Label Switching (MPLS) wide area networks (WAN) provide most of the long distance connectivity today and as such are replacing multiple older technologies such as Frame-Relay, X.25 or leased lines. MPLS provides quite similar functionality to its predecessors through the creation of separate, isolated communication paths based on different labels. Traffic isolation however provides no confidentiality nor authentication of the data traveling the MPLS network and opens the data to multiple risks when traveling over a shared infrastructure, such as e.g., possible data leak due to configuration errors or even illegal tapping.

3. *Encryption Options*

It is obvious throughout the history of communication protocols that protection of data while traveling over unsecured data channels could be achieved with encryption. However, encryption has proven to be a difficult task as it requires multiple other elements to be done correctly as well so as not to impact modern data communication networks. As we have described above, encryption impacts the performance, redundancy and load balancing of

modern day networks and also the requirement for any type of group communications is making the use of encryption problematic. Furthermore, there have been several options of where to implement encryption: on the link level, network level or application level. Let's browse through them briefly to see the pros and cons of each.

3.1. Link Level Encryption

Link Level Encryption was one of the earliest ones available and had no demand for standardization as there always was a product of the same vendor on both sides of the link. Key management protocols were often also proprietary and built in as part of the solution. Therefore, the price of such devices was high and when a device failed in a point-to-point topology both had to be replaced. The problems for link level encryption came with new network media connectivity options such as mesh topologies as well as multiple different paths through the same media. This led to the option of developing encryption on other levels, such as at the application or network levels.

3.2. Application Level Encryption

Application level encryption is from a security standpoint, the highest one - as the application that produces the data has the best visibility on how to protect it. It would be great if each and every application had the encryption possibility built in, however, as security was in the past often not the issue - many legacy applications stayed without it and have no option to turn it on. Newer applications mostly have the option to protect the data via encryption, however each and every one of them mostly has its own different way of how to do it, and that makes scalability as well as intra application data protection transfer impossible or non scalable.

3.3. Network Level Encryption

Due to the limitations and drawbacks of the other previously mentioned options and levels to encrypt the data, the network layer ended up as the most frequent choice. Network level encryption provides for equal protection to legacy applications as well as new applications traversing the same network protocol and requires no other application changes. As the most dominant network communication protocol today became Internet Protocol (IP), we will narrow our discussion on the encryption features within IP with its security protocol framework named IP security or shortly IPSec. The IPSec protocol got standardized a decade ago and through numerous interoperable implementations, prices of IPSec based equipment have become much more affordable than link level encryption devices used to be, but as usual it has its advantages as well as its limitations that we'll focus on going forward.

4. *Limitations of the IPSec encryption*

The IPSec set of Request for Comments (RFC) standards defined the authentication as well as encryption of the IP packet. It also defined different modes of operation as well as the Internet Key Exchange (IKE) automated key derivation protocol that helps with exchanging the keys based on a pre-defined time interval or amount of transferred data. Both together, IKE and IPSec got wide implementations on routers, layer three switches and edge devices such as firewalls as well as end nodes running on different operating systems. With wide implementations however, IPSec and IKE have also introduced new limitations. IPSec and

IKE are by definition a peer to peer protocol that impacts network communication if there are redundant paths or if load balancing is involved. Peer to peer trusted relationships also make encrypted group communication very difficult. This is illustrated in Exhibits 1 and 2. Last but not least if not implemented in hardware, certain encryption processes also impact the performance of the communication on any higher speed network connections.

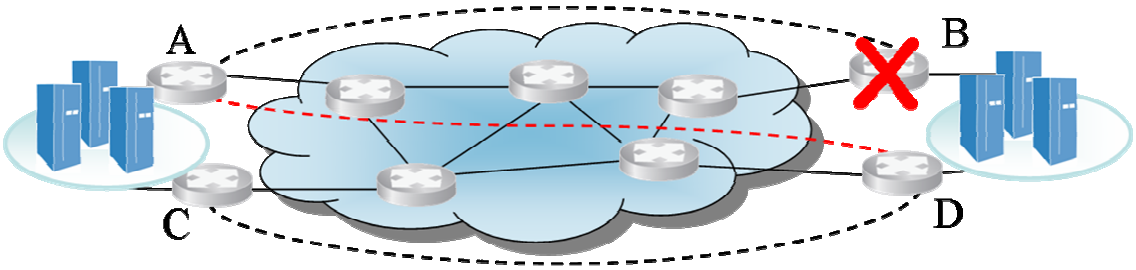

Exhibit 1: Redundant Network Architecture

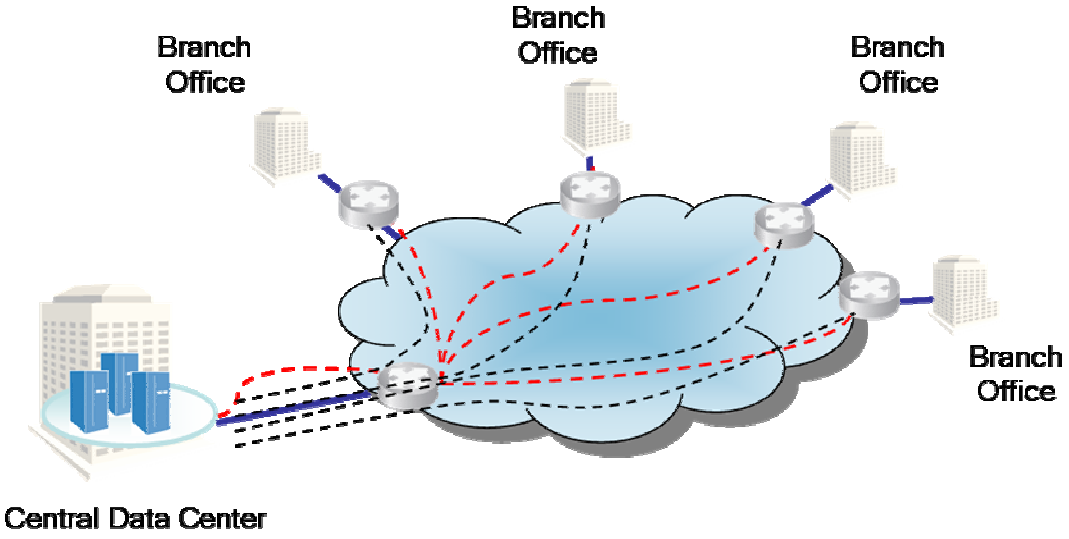

Exhibit 2: Group (Multicast or Broadcast) Network Architecture

5. *Separation of the Key Management Solution*

IPSec and IKE together represent three main functions most often implemented together in the very same, single running platform. These three functions are: Security Policy Definition, Key Exchange and Encryption. The most common implementation for all three functions as one IPSec/IKE architecture is illustrated in Exhibit 3.

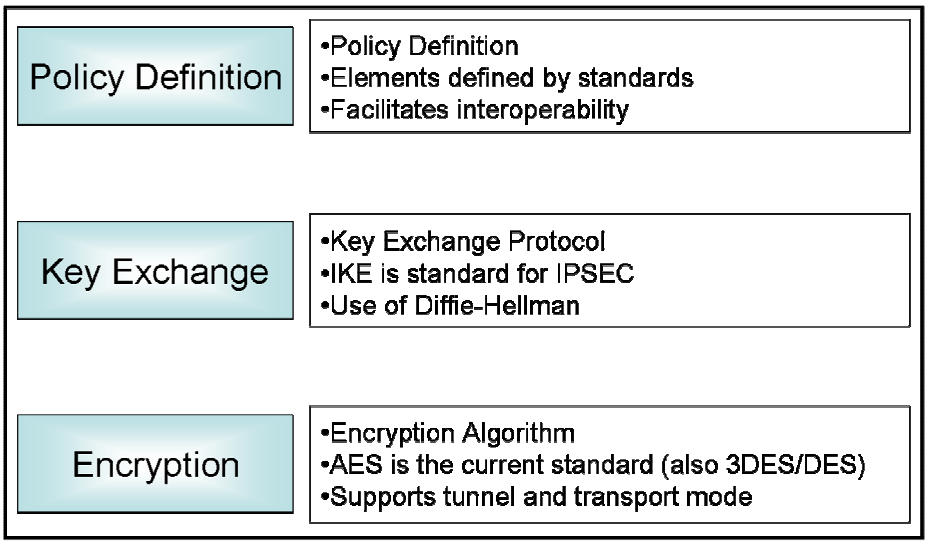

Exhibit 3: IPsec/IKE Common Architecture

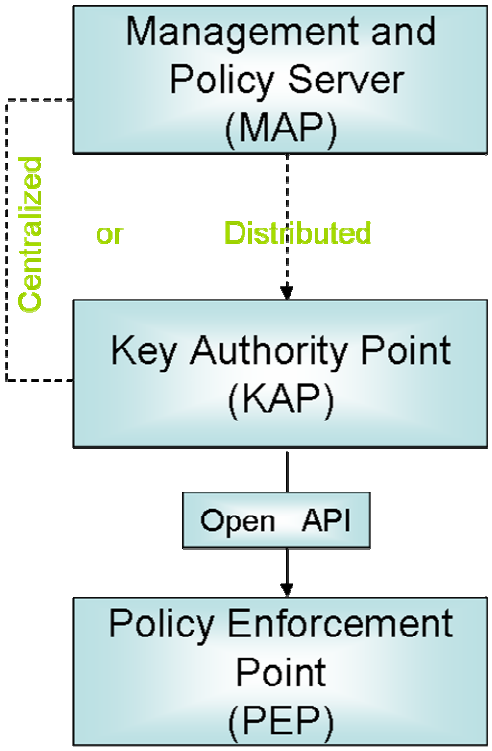

Exhibit 4: Distributed Policy and key Management Architecture

Implementation of all three of the main encryption components on the same physical platform seems to be an obvious choice, however it brings with it its limitations of peer to peer relationships and, therefore, impacts modern network communications. To be able to achieve resilient and redundant network designs, the encryption security architecture should have its components designed the same way. The three main components in essence represent three individual roles: bulk encryption - that could be done on the Policy Enforcement Point (PEP),

key management - that a Key Authority Point could take care of and security policies - that could be done on a Management and a Policy Server (MAP). This distributed model represented by the three individual layers: Management, Distribution and Encryption is illustrated in Exhibit 4.

Each of the main functional components could hence fulfill its job when implemented on individual platforms, thereby also bringing additional benefits such as scalability. Each of the layers in the three tier model could be replicated up to the necessary service scale level and support growth as required for large scale network designs. The Three Tier Security Architecture is illustrated in Exhibit 5.

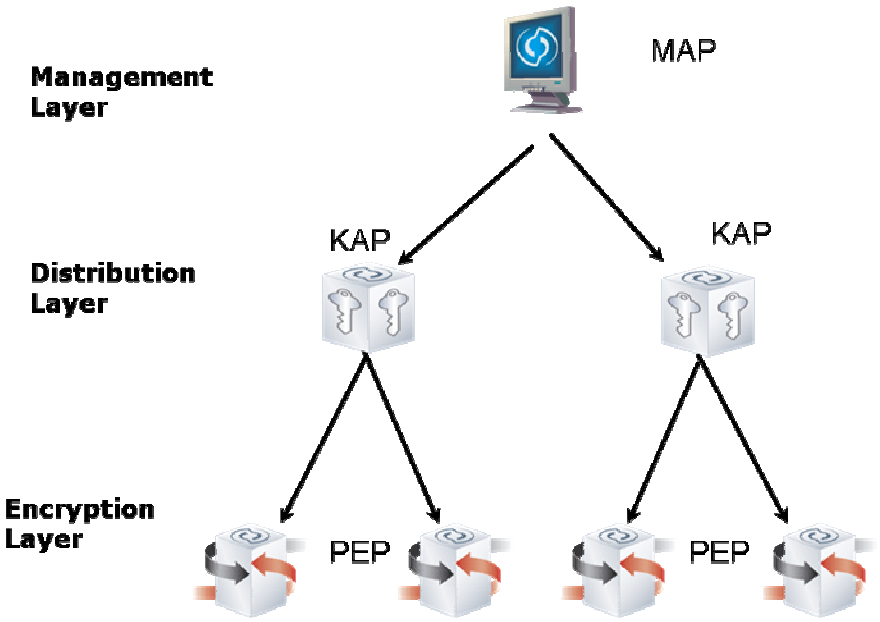

Exhibit 5: Three Tear Encryption Security Architecture

The key distribution layer and policy distribution layer have to be designed with redundancy and failover mechanisms as well as incorporate hardware security modules for key generations. The key storage has to be a “hack-proof” system with no backdoor and no possible traffic probing vulnerabilities. An additional problem to solve is security of the traffic between the layers. That could be resolved by utilizing either IKE or other secure but less heavy protocols, such as for example the Transport Layer Security (TLS) protocol. Scaling in such a distributed model is built in from the ground up by design. The three-layer architecture allows scalability of security policies never before possible using IPSec. Grouping networks and network device units together through group policy definitions dramatically simplifies policy generations. Therefore, the layered encryption security architecture can serve many thousands of end node policy enforcement points in the network and as well through the open API (Application Programming Interface) API provide access to hundreds of thousands of multi vendor devices, such as desktops, notebooks, cell-phones, PDAs, printers etc.
An additional element that helps break the point to point relationship is that Policy Enforcement Points responsible for the bulk encryption doing IPSec - maintain the original IP address header as is illustrated in Exhibit 6.

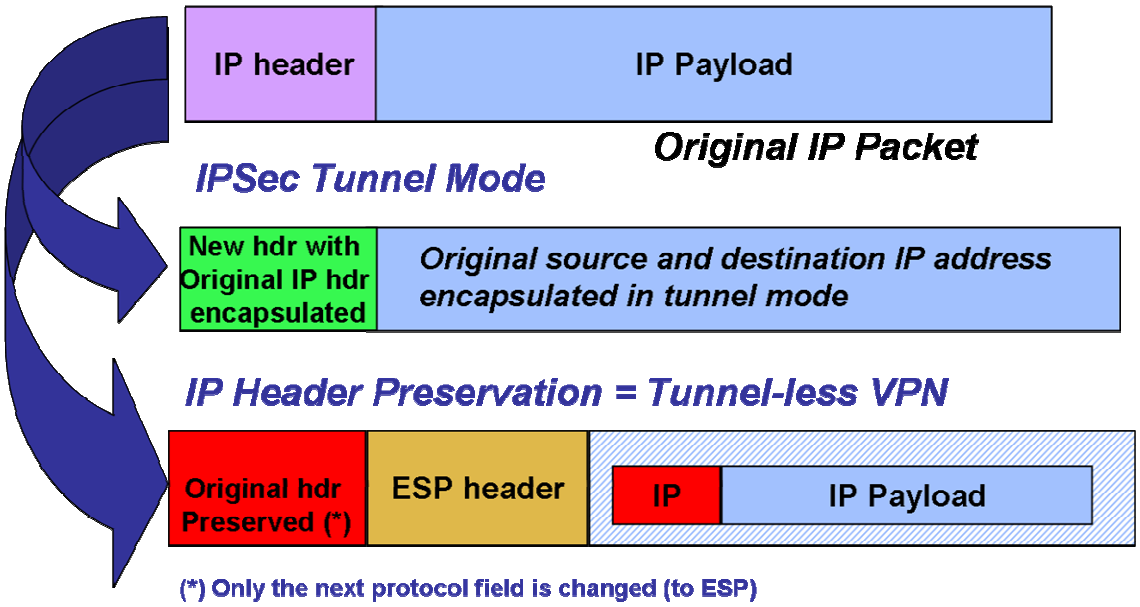

Exhibit 6: IPsec Tunnel Mode Header Preservation

With the original IP header preserved, there is no additional need to create any point to point relationships and even more important, no need to create any overlay network on top of existing infrastructure. That simplifies the encryption function on the existing modern networks to the maximum possible and as such only adds flexibility to enabling redundancy, load balancing as well as group broadcast or multicast communication.

6. *Summary*

The challenge in front of the information security professionals is to secure data in motion like never before. Encryption is the obvious choice for the solution but the solution must work over any network topology and must secure any type of traffic. All of that has to be preferably done without requiring changes to the network infrastructure or impacting the network performance. The IPSec protocol brings us part of the solution but is also part of the problem with its point to point nature as well as the network overlay model. A layered encryption security architecture brings a solution to the requirements of modern data protection through the separation of the main roles and functions of encryption into three individual layers. Such a three tier encryption security architecture brings inherited scalability and does no longer require a network overlay for the generation and distribution of policies and encryption keys. It provides data protection but does not require any changes to network infrastructure, does not impact network performance and works over any network topology. It is a concept that should, once widely implemented, solve the problem of data protection through encryption in large scale network deployments.

7. *List of Acronyms*

API Application Programming Interface
IETF Internet Engineering task Force
IKE Internet Key Exchange
IPSec IP Security
KAP Key Authority Point
MAP Management and Policy
MPLS Multi Protocol Label Switching
PEP Policy Enforcement Point
RFC Request For Comment
WAN Wide Area Network

8. *References*

[1] Bauger M., Weis B., Hardjono T., Harney H., The Group Domain of Interpretation, RFC3547, IETF Standard, July 2003.

[2] Carlton R. Davis, IPSec: Securing VPNs, McGraw- Hill 2001.

[3] Doraswamy N., Harkins D., IPSec The New Security Standard for the Internet, Intranets and Virtual Private Networks, Prentice Hall PTR 1999.

[4] Ferguson, N., Schneier, B., A Cryptographic Evaluation of IPSec, <www.counterpane.com/ipsec.html>, Apr. 1999.

[5] Frankel, S., Demystifying the IPsec Puzzle, Artech House Inc., 2001.

[6] Harkins D., Carrel D., The Internet Key Exchange (IKE), RFC 2409, November 1998.

[7] Kent, S., Atkinson R., Security Architecture for the Internet Protocol, RFC 2401, November 1998.

[8] Kent, S., Atkinson R., IP Authentication Header, RFC 2402, November 1998.

[9] Kent, S., Atkinson R., IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

[10] Kosiur D., Building and Managing Virtual Private Networks, Willey Computer Publishing 1998.

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

[12] Perlman, R., Kaufman, C., Key Exchange in IPSec: Analysis of IKE, IEEE Internet Computing Vol. 4, No.6; p50-56, November-December 2000.

[13] Perlman, R., Kaufman, C., Analysis of the IPsec key exchange Standard, WET-ICE Security Conference, MIT, <sec.femto.org/wetice-2001/papers/radia-paper.pdf>, 2001.

[14] Weis B., Hardjono T., Harney H., The Multicast Group Security Architecture, RFC 3740, IETF Standard, July 2004.

[15] Weis B., Gross G., Ignjatic D., Multicast Extensions to the Security Architecture for the Internet Protocol , IETF draft RFC <draft-ietf-msec-ipsec-extensions-04.txt>