VIRTUAL PRIVATE NETWORKS (VPN) APPLICATIONS AT SAUDI ARAMCO

Khalid Bin-Rashid, Saudi Aramco

Abstract:

This technical paper explains the Virtual Private Networks (VPN) technology, and its possible deployments by organizations, particularly Saudi Aramco. VPN have advanced tremendously in the last couple of years especially with the ever-increasing demand for e-business and the widespread deployment of the Internet.

1. Introduction:

Saudi Aramco has built a magnificent Intranet that posts tremendous amount of information mostly proprietary for its employees. Also, Saudi Aramco has installed secure and powerful servers for its mission critical and business applications. Most of Saudi Aramco offices In-Kingdom are connected to its Intranet using its own communications network. Some local and all of Out-of-Kingdom offices use costly leased circuits to connect to its Intranet. Saudi Aramco employees are accustomed in utilizing these networking resources to do business, and are becoming more dependent on them on their daily work. Employees can access Saudi Aramco Intranet from home using either dial-up with SecurID pass or dial-back services. Employees traveling in short business assignments cannot connect to Saudi Aramco Intranet unless they use very costly international or long-distance telephone calls along with their SecurID pass.

Virtual Private Networks (VPN) can be implemented by organizations to avoid the costly leased circuits and international calls. VPN use a public network like the Internet to securely connect private users and networks. VPN implementation uses IPSec which is the Internet Engineering Task Force's (IETF) Internet Protocol (IP) Security (IPSec) Standard. It is composed of a collection of Internet Request For Comments (RFCs) that address the confidentiality, integrity, authentication, and access control of IP packets. The collection includes standards for encryption and authentication, as well as standards for key exchange. IPSec can be viewed as creating a tunnel between two end points in the network. To setup a VPN between two sites, an IPSec tunnel needs to be implemented between them.

Saudi Aramco Out-of-Kingdom offices and project offices can use their local Internet connection at their locations to build VPN to communicate securely with Saudi Aramco Intranet. Traveling employees can use any local Internet Service Provider (ISP) to connect to the Internet and then build VPN with Saudi Aramco Intranet to obtain specific documents or data. On the other hand, to streamline its business and operation Saudi Aramco can build VPN with its partners, suppliers, and even its customers.

This technical paper will define and describe VPN components and setup configuration, and will give an overview of how VPN are implemented. Site-to-site VPN implementations are to be used to interconnect two offices using the Internet. User-to-site VPN implementations are to be used by traveling employees to access their companies Intranet using the Internet. This paper will also discuss briefly the user authentication methods used in VPN, like Public Key Infrastructure (PKI), which is best to be used with VPN and ease VPN scalability. It will point out some of VPN setup oversights that can lead to poor VPN implementations.

2. VPN Overview:

VPN can be simply defined as using a public network and encryption to build a private network, see figure 1. VPN shall meet the following challenges:

- Data Integrity; i.e. no one in the public network can alter the data transmitted.
- Message Privacy; i.e. no one in the public network can read the information.
- Authentication; i.e. further assurance that no one pretends to be another trusted.
- Access Control; i.e. restricting access to only those services approved for the user.
- Audit and Logging; i.e. recording all VPN events, for accounting and recovery.
- Quality of Service; i.e. at the future, guarantee bandwidth end to end.

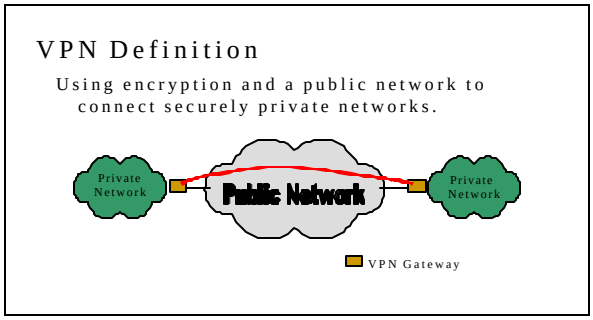

Figure 1: VPN Simplified Schematic Diagram.

VPN advantages are:

- Reduce Cost by eliminating the usage of costly long distant dialup and leased circuits.
- Increase Security by applying stringent encryption and authentication techniques.
- Integrate Data by allowing branch offices have access easily to the head office network and data.
- Simplify Operation; i.e. it takes less time to setup VPN than acquiring a leased circuit.
- Scalability.

There are three types of VPN implementation:

- Internet; where the Internet is used as the public media, for one company network, see figure 2.
- Intranet; where the Intranet is the public media, so it is internally implemented, see figure 3.
- Extranet; where the Internet is the public media, for different companies networks, see figure 4.

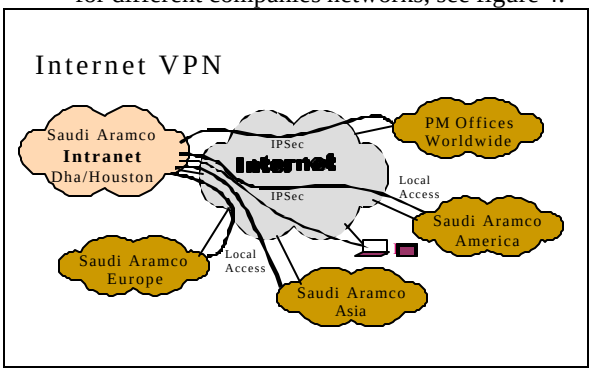

Figure 2: Internet VPN Implementation.

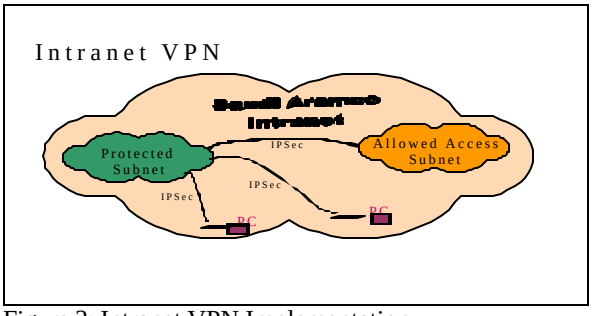

Figure 3: Intranet VPN Implementation.

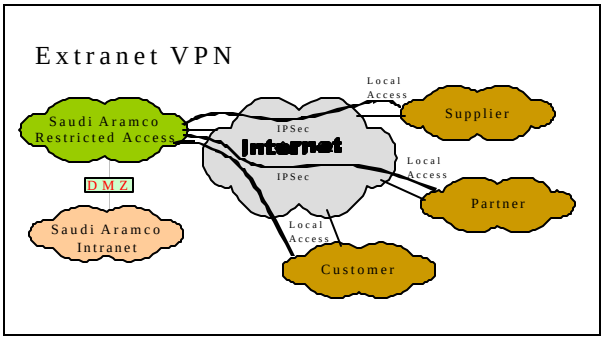

Figure4: Extranet VPN Implementation.

3. VPN Types:

There are two types of VPN. Gateway-to-gateway uses IPSec Tunnel Mode, where the original sender and receiver IP addresses are encrypted within the transmitted IP packets that use two new IPs of the IPSec tunnel end points, i.e., VPN gateways. And, client-to-gateway that uses IPSec Transport Mode, where the original IPs are sent in the clear. Both types can be established either statically or dynamically. Static VPN are setup by manually entering the various encryption and authentication keys. Dynamic VPN use automated systems that generate all keys.

IPSec consists of two protocols that can be used either individually or combined: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data integrity, but no confidentiality, by applying a hash function, like MD5 or SHA-1, to the whole IP packet and attaching the result to the transmitted data. The hash function takes any input (up to 2^{64} bit), applies the specified algorithm using a seed or agreed upon key, and generates a fixed length message digest. The receiver apply the same hash function using the same key and compare with the attached digest, if the result is the same then there was no alteration to the original data.

ESP provides both integrity and confidentiality by applying a hash function and a symmetric encryption algorithm, like DES and triple-DES, to encrypt the sent data. Symmetric Encryption uses one secret key to do both encryption and decryption. They are very fast compared with public key encryption, but the secret key must be exchanged very securely.

3.1. Static VPN:

They use static IPSec tunnels which configurations rely on manually created and entered authentication and encryption secret keys. The problem with this type is the hassle of ensuring that all keys are handed to the two ends in a very secure way. So, key management must be implemented as new set of keys must be developed and distributed every time it feared the used keys are compromised, or they have been used for a long time. When there are many tunnels with different parties the management of keys becomes troublesome as unique set of keys should be used with each party, and these keys must be updated frequently.

To setup static VPN a static IPSec tunnel needs to be configured between two networks. The Tunnel End Point (TEP) IP addresses of the VPN gateways and the IP segments that will be allowed access behind each gateway need to be identified. Two security associations are needed for each IPSec tunnel, one for each direction, i.e. inbound and outbound. A unique Security Parameter

Index (SPI) identifies each security association and needs to be entered. The IPSec protocol (AH and/or ESP) needs to be specified. The authentication algorithm and the secret key need to be entered. The encryption algorithm and the secret key need to be entered. The last is to specify the services allowed in and out, like ftp, http, and e-mail.

This is error-prone as it is easy to make a mistake when entering any of the 16-to-42 hex-digit secret keys. Some VPN gateways are configured in hexadecimal while others in decimal, which further complicate the static IPSec configuration. VPN scalability is limited with the use of static IPSec because of the troublesome of managing all keys especially when deployed among different companies. It is, however, required by standard to ensure workability between any two different VPN gateways.

3.2. Dynamic VPN:

Here all keys are created by the electronics using algorithms like Key Management Protocol (KMP) and Internet Key Exchange (IKE) to create, agree on, and exchange the secret keys. They rely on public key encryption algorithms like RSA, which use two keys: a public key to encrypt with and a private key to decrypt with. They are only used to exchange all dynamically generated authentication and encryption secret keys in a secure way. The secret keys will still be used for the IPSec tunnel authentication and encryption algorithms, like in the static IPSec. This is because secret key encryption is much faster (about 1000 times) than public key encryption.

To setup dynamic VPN a dynamic IPSec tunnel needs to be configured between two networks. The Tunnel End Point (TEP) IP addresses of the VPN gateways and the IP segments that will be allowed access behind each gateway need to be identified. Here only the IPSec protocol and algorithms need to be specified without any specific keys or values. The last is to specify the services allowed in and out, like ftp, http, and e-mail.

There are features that can be implemented with dynamic VPN only. New secret keys can be configured to be issued and used whenever a preset time (e.g. 6 hours) has elapsed on the usage of the previous secret keys while the IPSec tunnel still up. Or, when a preset volume (e.g. 100 Mbytes) of data traffic has traversed the IPSec tunnel. There is a keep-alive mechanism to ensure that the IPSec tunnel is properly up, so when the communications link goes down so does the IPSec tunnel and when the communications link comes up so does the IPSec tunnel. There is also a mechanism to allow one end to negotiate for a less stringent authentication or encryption algorithm if the other end does not support the specified algorithm.

VPN setup is much easier using dynamic IPSec than static IPSec, because it is simpler to configure dynamic IPSec as the fields to be entered are much less. It is also more secure to use dynamic IPSec tunnels as secret keys are regenerated frequently and per the volume and timer limits entered during the configuration. Troubleshooting dynamic IPSec tunnels is easier than the static. The static tunnels are presumed by the electronics to be up even when the communications link goes down, and there are no automated systems to ensure the status of static IPSec tunnels. On the other hand, the dynamic tunnels are continuously monitored to confirm their status, especially as the two end points renegotiate for new set of keys when preset limits expire.

4. User Authentication Types:

There are many methods to authenticate VPN users and gateways. Local passwords can be maintained by the VPN gateway to use for authenticating end users. VPN gateway can use a Lightweight Directory Access Protocol (LDAP) server to authenticate users. Authentication, Authorization, and Accounting (AAA) server like Remote Authentication Dial-In User Service (RADIUS) can be used. Other examples include TACACS+ and SecurID, see figure 5.

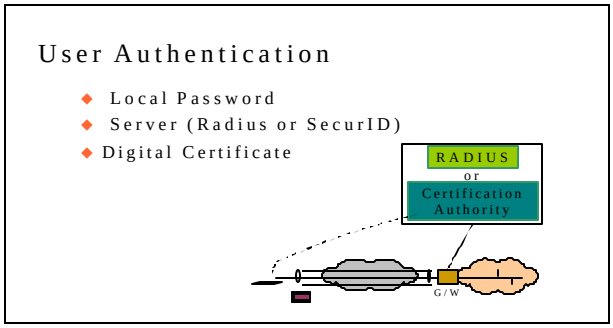

Figure 5: VPN User Authentication Methods.

However, the best is to use Digital Certificates (DC) for authenticating both end users and VPN gateways. Digital certification relies on Public Key Infrastructure (PKI) and Certification Authority (CA) to issue and distribute DC. A DC gives more stringent authentication than a password or a SecurID. It includes fields when properly used will greatly simplify VPN deployment, eliminating the need to include in the VPN configuration any secret pre-shared keys. The company will not need to safeguard any secret keys and will easily setup VPN with any party that holds a DC trusted by it. This will ease VPN scalability.

There are two options, a company may either have an internal unit acting as a CA to issue DC's for its users and equipment as well as others, or lease from another agency the needed DC's. When a CA issues a DC for someone it vows to whoever has the CA public key that

the DC belongs to that specific someone. The CA verifies credentials before issuing any DC. The DC usually contains the person's or device name, their public key, the CA signature of the key, and an expiration date. X.509 standard addresses the DC fields, which uses X.500 naming standard. On the other hand, the CA maintains a Certificate Revocation List (CRL) to include all DC's that are cancelled by the CA before their end time. After a VPN gateway verifies a DC, it checks also the CA's CRL to ensure it is not revoked, before establishing the IPSec tunnel.

VPN implementation becomes easier and more scalable when used with digital certification. VPN gateways can be configured to setup IPSec tunnels with all who have trusted DC with a specific value of field, for example with Subject Name: c= SA, o=Saudi Aramco, ou=IT (where c stands for country, o for organization, and ou for organizational unit). The two end VPN devices can use the authentication and encryption algorithms specified on the DC's for the IPSec tunnel.

5. VPN Deployment:

Before a company can deploy VPN, it first needs to update its network security policy to clarify all access restrictions for its employees, contractors, partners, suppliers, and customers. The company needs also to decide on the best user authentication method to use for its VPN deployment, keeping in mind that digital certificates are the most stringent authentication scheme. It needs to evaluate the VPN manufacturer products available in the market to select the products family that meets its needs. This will simplify VPN deployment as its engineers and technicians need only to learn one-manufacturer configuration procedures. It helps to specify a set of VPN design guidelines so engineers can easily follow.

Saudi Aramco branch and project offices worldwide can use only one local connection to the Internet to provide secure VPN links with Saudi Aramco headquarter, project contractors, and major suppliers. This will streamline operations by not only getting connected faster than acquiring the needed leased circuits, but also simplify network connectivity by using only one piece of equipment for one link to communicate with various parties. On the other hand, Saudi Aramco head office will need to maintain less remote access equipment (modems) to connect its remote users. Users will use the Internet and VPN to communicate with the head office through the companies Internet router and/or VPN gateway.

VPN can be used as an emergency reroute when a leased circuit between two major sites gets interrupted. The VPN link relying on the Internet diverse routes can be turned up, as traffic most likely will use another Internet link. There is no bandwidth or quality of service guarantees at this time for VPN implementations unless they are deployed using one carrier or service provider network with the desired service level agreement.

6. Conclusion:

VPN implementation will increase as the need to reduce communication cost and enable e-business increase. VPN utilize the local Internet connection to establish secure communication links with branch offices, partners, suppliers, and customers. This simplifies network connectivity by using the local Internet connection to communicate to everywhere. Site-to-site VPN are to interconnect office networks, while client-to-site VPN are to interconnect users to office networks.

It is best to use automatic VPN using dynamic IPSec tunnels to increase network security and scalability. Using an AAA server or digital certification will augment and ease VPN implementation.

Reference:

1. Keith Carduck, *Lucent's* Managed Premises VPN Offer Release/Implementation Notes, Issue 1.0, March 2000.
2. Security Architecture for the Internet Protocol, IETF RFC 2401.
3. IP Authentication Header, IETF RFC 2402.
4. IP Encapsulating Security Payload, IETF RFC 2406.

Biography:

Khalid Ali Bin-Rashid, RCDD, PMP, born in 1967 and raised at Dammam, Saudi Arabia. He earned B.S. in Electrical Engineering from KFUPM on 1989, and M.S. in EE from University of Portland on 1996. Currently Khalid works for Saudi Aramco, since March 1991, as a data communications engineer at the IT Computer and Communications Engineering Department. He was assigned one year from July 1999 to June 2000 with Lucent's Bell Laboratories during which he worked on the interoperability testing of Virtual Private Networks (VPN) products.