A Study on IP Virtual Private Network Architecture

Rosslin John Robles*, Nayoun Kim*, Feruza Sattarova*,
Seok-soo Kim*, Tai-hoon Kim*
*Dept of Multimedia Engineering, HanNam University
e-mail:rosslin_john@yahoo.com

A Study on IP Virtual Private Network Architecture

로즐린 존 노블레스*, 김나윤*, 페루자 산타로바*, 김석수*, 김태훈*
*한남대학교 멀티미디어공학전공

Abstract

A VPN is a private network that uses a public network to connect remote sites or users together. As its popularity grows, companies, organization and even the government turned to it as a means of extending their own networks. To setup a Virtual Private a proper IP VPN Architecture must first be selected. In this paper, the types of IP Virtual Private Network Architecture like the MPLS-Based, IPSec-Based and the SSL/TLS-Based are discussed and compared. The comparison may serve as a guide for selecting the proper IP Virtual Private Network Architecture that is suitable for the company's needs.

1. Introduction

As the internet became popular, companies, organization and even the government turned to it as a means of extending their own networks. The first that were used are the intranets, which are password-protected sites designed for use only by company employees. Today, many companies are creating their own VPN (virtual private network) to accommodate the needs of remote employees and distant branch offices.

A VPN is a private network that uses a public network (like the Internet) to connect remote sites or users together. As an alternative to dedicated, real-world connection such as leased line, a virtual private network uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. [1] Virtual private networks help distant colleagues work together, much like desktop sharing.

[Fig. 1] Virtual Private Network diagram

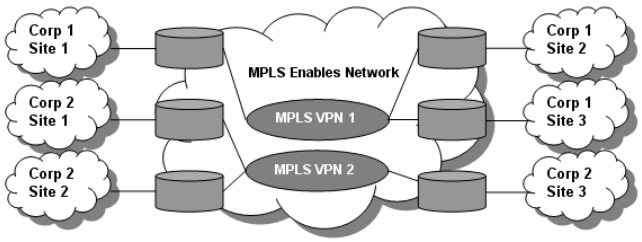
An IP VPN is a partitioned private network constructed over a shared IP-based backbone that utilizes technologies to ensure privacy of data. They offer enterprise-class scalability and reachability across multiple IP-based infrastructures, along with many of the performance and security characteristics traditionally found only in dedicated private environments. [2]

2. IP VPN Architecture

There are many kinds of IP VPN architectures and selecting IP VPN architecture is crucial. The Optimal IP VPN depends on the companies requirements. The IP VPN architecture selected by the company has a wide-ranging effect on business, including connectivity options, scalability, and the ability to deploy video, voice, and multicast applications. [3] The types of IP VPN architectures are discussed on the next part of this paper.

2.1 MPLS

MPLS Virtual Private Network is a method for harnessing the power of Multiprotocol Label Switching to create Virtual Private Networks. MPLS is designed to the task as it provides traffic isolation and differentiation without substantial overhead. [4] As seen in figure 2, the primary advantage of MPLS is that it provides support to both small and very large-scale VPN deployments: up to tens of thousands of VPNs on the same network core. Aside from scalability, its benefits include end-to-end QoS, rapid fault correction of link and node failure, bandwidth protection, and a foundation for deploying additional value-added services. MPLS technology also simplifies management, configuration, and provisioning, helping service providers to deliver highly scalable, differentiated, end-to-end IPbased services. Since it is a network-based VPN service, MPLS don't require the use of a VPN client. Enterprise end users typically interact with the network as they would ordinarily. [3]



[Fig. 2] MPLS-Based Virtual Private Network

Multiprotocol Label Switching Virtual Private Network have the following advantages:

- Network security —MPLS enforces traffic separation between different VPNs on the same core network by using route distinguishers.
- Support for SLAs —Service Level Agreements or SLAs are important to enterprises with stringent requirements for network resiliency and performance.
- Scalability —MPLS-based VPN deployment scales easily to undergo company growth or changes.

2.2 IPSec

Internet Protocol Security is a suite of protocols for securing Internet Protocol communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. [5]

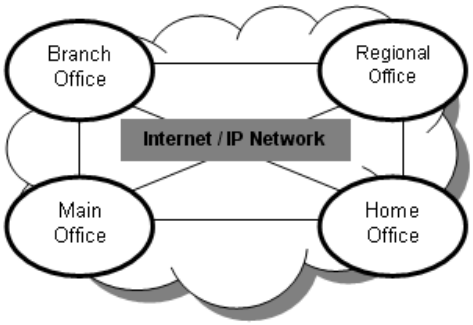
The advantages of IPSec-based VPN for the enterprise are:

- Low cost
- Ease of deployment
- Strong security
- Support for teleworkers and mobile workers
- Reduced congestion at hub site

IPSec supports a combination of the following network security functions: Data origin authentication, Data confidentiality, Data integrity and Antireplay. IPSec is suitable for both site-to-site and remote-access Virtual Private Networks.

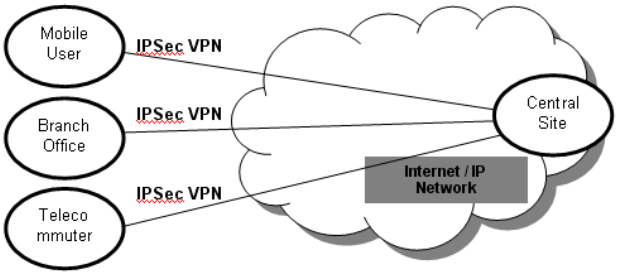
Typically in a Remote access setup, the user runs the VPN software client and selects the appropriate destination, like host name or IP address. After successful authentication and IPSec

tunnel setup, users can access applications as they would from their offices. IPSec allows access to almost all networked applications, without any modifications to the hosted site or client.



[Fig. 3] IPSec-Based Virtual Private Network

In the case of site-to-site connectivity via an IPSec-based VPN, users do not need client software on their computers. Rather, the user at a branch office launches the application as if it resided locally. An IPSec-enabled VPN router at the branch office automatically initiates an IPSec session with the central office. If a session negotiation and authentication is successful, a secure VPN tunnel is established between the branch and central office, without any action by the user.



[Fig. 4] Remote Access IPSec Virtual Private Network

2.3 SSL/TLS

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. [6] Secure Sockets Layer (SSL) is an emerging alternative to IPSec for remote-access VPNs. It is not designed for site-to-site VPNs. [3] An advantage of SSL as a remote-access Virtual Private Network is that it does not require any special VPN client software other than a Web browser. Also, the enterprise IT group or service provider can provide granular access control, limiting access to specific Web pages or other internal resources.

The advantages of SSL for secure remote access include:

- Support for existing and planned authentication methods
- Provides "anywhere access"
- Low training overhead
- Reduces network interoperability issues
- Transparent wireless roaming
- Client ubiquity

3. VPN Architecture Evaluation Measures

The IP VPN function is to provide cost-effective, secure connectivity over a shared infrastructure with the same or better policies and service attributes that the enterprise enjoys within its dedicated private network. To accomplish this, the IP VPN solution should deliver the following essential attributes: high availability, network security, quality of service, and ease of management. IP VPN architecture types deliver different advantages to the enterprise, so it is up to them to select which architecture suites their needs.

4. Comparison of the architecture

4.1 Topology and Place in network

In MPLS, the topology that is used is Site-to-site VPN (Hub-and-spoke or full-mesh) and uses the core network as its place in network. In IPSec-Based VPN, Site-to-site VPN (Mainly hub-and-spoke). An in SSL-Based VPN, Remote-access VPN is used. Both SSL-Based VPN and IPSec-Based VPN utilize local loop,

edge, and off-net as place in network

4.2 Security

In terms of session authentication, MPLS-Based VPN Establishes VPN membership during provisioning, based on logical port and unique route descriptor Defines access to a VPN service group during service configuration; denies unauthorized access. While IPSec-based authenticates through digital certificate or preshared key and drops packets that do not conform to the security policy. SSL-based VPN authenticates through digital certificate

In terms of confidentiality, MPLS-Based VPN separates traffic, which achieves same results delivered in trusted Frame Relay or ATM network environments. IPSec-Based VPN uses a flexible suite of encryption and tunneling mechanisms at the IP network layer. While the SSL-based VPN Encrypts traffic using the public key infrastructure (PKI).

4.3 VPN client

In MPLS-Based VPN, a VPN client is not required because MPLS VPN is a network-based VPN service; users do not need VPN clients to interact with the network. In IPSec-Based VPN, a VPN client is required for client-initiated IPSec VPN deployments Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems. While is SSL-Based VPN, it is not required since it only relies on the browser.

5. Conclusion

This paper discusses the types of IP Virtual Private Network Architecture, their setup and the advantages that they may bring. The IP VPN architecture selected by the company has a wide-ranging effect on business, including connectivity options, scalability, and the ability to deploy video, voice, and multicast applications, [3] therefore selecting a proper IP VPN Architecture is very crucial. This study is designed to help companies to select which architecture or combination of IP VPN architecture is suitable for their needs.

References

[1] Jeff Tyson "How Virtual Private Networks Work"
http://computer.howstuffworks.com/vpn.htm Accessed: February 2009

[2] SLK "What is IP VPN"
http://www.slt.lk/data/forbusiness/101ipvpn.htm Accessed: February 2009

[3] Cisco Systems, Inc. White Paper (2004) "Enterprise Guide for Selecting an IP VPN Architecture"

[4] Wikipedia - MPLS VPN
http://en.wikipedia.org/wiki/MPLS_VPN Accessed: February 2009

[5] IP Security Protocol Official Charter, *Internet Engineering Task Force (IETF)* http://www.ietf.org/html.charters/OLD/ipsec-charter.html Accessed: February 2009

[6] Wikipedia - IPSec
http://en.wikipedia.org/wiki/IPsec Accessed: February .2009