

IP Based Virtual Private Network Implementation on Financial Institution and Banking System

Dr. Amir Hassan Pathan and Muniza Irshad
amir.pathan@sbp.org.pk and mcsit_muniza@yahoo.com
SZABIST, Karachi, Pakistan

Abstract: The aim and objective of this research paper is to propose Secured Network Model based on VPN Technology that will contribute the security requirement of the Financial Institution and Banking System.

1 INTRODUCTION

1.1 Security Architecture

The security architecture is typically integrated into the existing enterprise network and is dependent on the IT services that are offered through the network infrastructure.

The architecture should define common security services to be implemented across the network.

- 1) *Identity:* Password authentication, authorization, and accounting (AAA)
- 2) *Secure Connectivity:* Confidentiality provided by virtual private networks (VPNs)
- 3) *Perimeter Security:* Access (trust model)
- 4) *Security Monitoring:* Security monitoring by intrusion detection systems (IDSs)

1.2 Secure Connectivity

Confidentiality provided by virtual private networks enterprises can establish private, secure communications across a public network. Usually the Internet and extend their corporate networks to remote offices, mobile users, telecommuters, and extranet partners.

Virtual Private Network allows one of outside user access to certain area of the intranet. Virtual Private Network is simply a private network that has been extended across a shared network or across a public network like the Internet.

1.3 Two Types Of Virtual Private Networks

There are two types of Virtual Private Networks.

- Site-to-Site Virtual Private Networks
- Remote-access Virtual Private Networks.

Site-to-Site VPNs encrypted VPNs provide the same benefits as a private WAN, ensuring private communication from one trusted site to another, providing multiprotocol support, high reliability, and extensive scalability. In addition Site-to-Site encrypted VPNs are cost-effective, secure, and allow for greater administrative flexibility than legacy private WANs.

Remote-access VPNs connect telecommuters, mobile users, or even smaller remote offices with minimal traffic to the enterprise WAN and corporate computing resources. [1]

1.4 Encryption Technology

Encryption technology ensures that messages traveling across a VPN cannot be intercepted or read by anyone other than the authorized recipient by using advanced mathematical algorithms. [1]

- IP Security (IPSec) Encryption
- Generic Routing Encapsulation (GRE)
- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Microsoft Point-to-Point Encryption(MPPE)

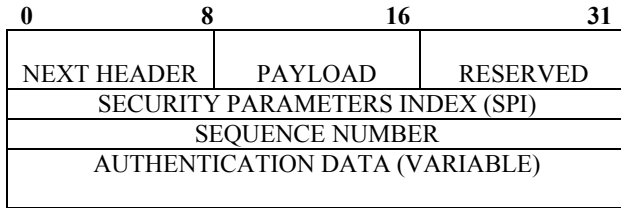
1.5 IP Security (IPSec) Encryption

IP Security (IPSec) encryption and tunneling technology to dynamically create a secure connection between the sending and receiving sites, tearing down the connection when the communication is completed.

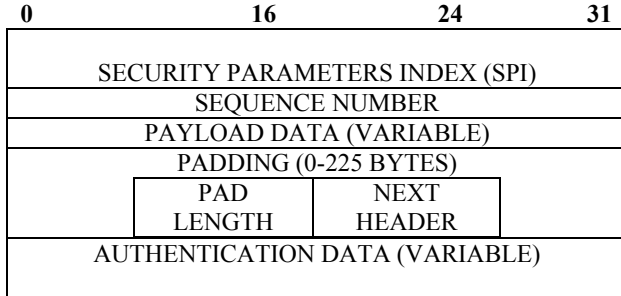
IP Security (IPSec) is a standard-based set of security protocols and algorithms. IPSec acts at the network layer, protecting and authenticating IP Packets between participation IPSec devices (peers) such as routers, Firewalls, VPN Client, VPN Concentrators, and other IPSec-compliant products. IPSec Based VPNs can be used to scale from small to large networks.

1.6 IP Security Architecture

1.6.1 Authentication Header



1.6.2 Encapsulating Security Payload



1.7 Security Association:

| IP Security Services | AH | ESP Encryption | ESP Encryption |
|-------------------------------|----|----------------|----------------|
| Access Control | ✓ | ✓ | ✓ |
| Connection Integrity | ✓ | | ✓ |
| Data Origin Authentication | ✓ | | ✓ |
| Rejection Of Replayed Packets | ✓ | ✓ | ✓ |
| Confidentiality | | ✓ | ✓ |
| Limited Traffic Flow | | ✓ | ✓ |

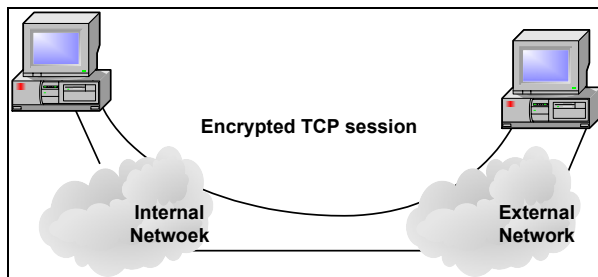
Table 1. Security Association

1.8 Transport and Tunnel Modes:

Transport Mode (Host To Host)

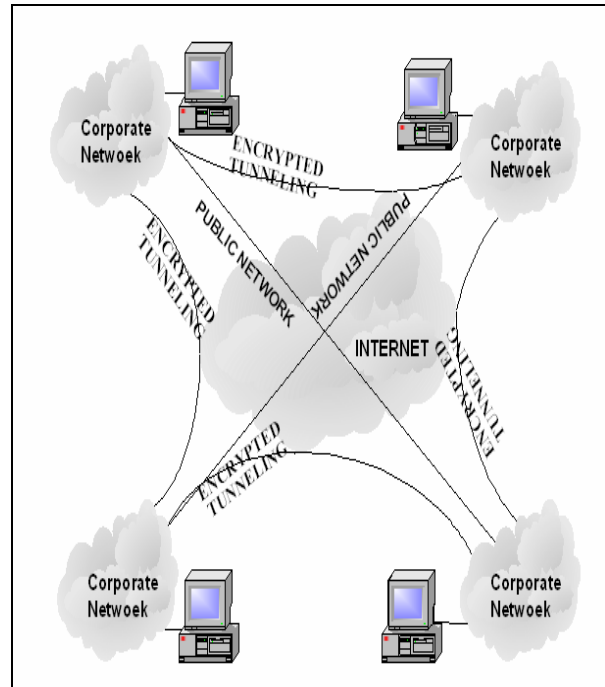
Figure 1. IP Security (IPSec) Encryption Technology.

Transport Level Security



Tunnel Mode (Router To Router)

Figure 2. IP Security (IPSec) Encryption And Tunneling Technology.



Tunnel Level Security

1.8.1 Transport Mode

Transport Mode provides protection primarily for upper layer protocols. Transport Mode extends to the payload of a packets .TCP or UDP segment, or an ICMP packet, all of which operate directly above IP in a host protocol stack. Typically, transport mode used for End-to-End Communication. [2]

1.8.2 Tunnel Mode

Tunnel Mode provides protection to the entire IP packet. After the AH & ESP field are added to the IP packet, the entire packet plus security field is treated as the payload of new "outer" IP packet with a new outer IP header. The original or inner packet travels through a "tunnel" from one point of an IP network to another. [2]

Table 2. Function Transport & Tunnel Mode

| Function | Transport Mode SA | Tunnel Mode SA |
|--------------------|---------------------------|--|
| AH | Authentication IP Payload | Authentication Entire IP Inner Packet |
| ESP Encryption | Encrypt IP Payload | Encrypt Entire IP Inner Packet |
| ESP Authentication | Encrypt IP Payload | Encrypt & Authentication Inner IP packet |

1.9 IP Security Services

- Access Control
- Connection Integrity
- Data Origin Authentication
- Rejection Of Replayed Packet
- Confidentiality
- Limited Traffic Flow Confidentiality[4],[5]

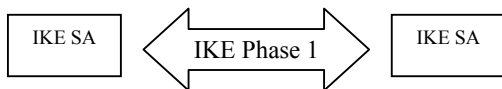
1.10 IPSec Process Flow

IPSec involves many component technologies and encryption methods and its operation divided into five steps: [6]

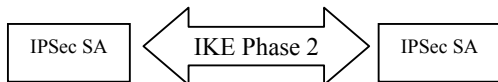
Step # 1 IPSec Process Initiation: -



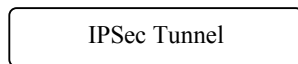
Step # 2 IKE Phase 1: -



Step # 3 IKE Phase 2: -



Step # 4 Data Transfer: -



Step # 5 IPSec Tunnel Termination: -

IPSec Works

- 1) *Step # 1 IPSec Process Initiation:* Traffic to be encrypted as by the specified IPSec policy configured in the IPSec peer starts the IKE process.
- 2) *Step # 2 IKE Phase 1:* IKE authentication IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.
- 3) *Step # 3 IKE Phase 2:* IKE negotiates IPSec SA parameters and setup matching IPSec SAs in the peers.
- 4) *Step # 4 Data Transfer:* Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA Database.
- 5) *Step # 5 IPSec Tunnel Termination:* IPSec SAs terminate through deletion or by timing out.

2. DATA CONNECTIVITY & SECURE CONNECTIVITY

Role of Service Provider in Pakistan:

2.1 Pakistan Telecommunication Co. Ltd.

2.1.1 Corporate Customers Services.

PTCL offer the following Services to Corporate Customers: [7]

UAN (Universal Access Number), UIN (Universal Internet Number), Toll Free (0800), Premium Rate Services (0900), Digital Cross Connect (DXX), TelePlus (ISDN BRI), Virtual Private Network (VPN), Facility for Call Centres, Tele Mail, Co- location Centres, Digital Subscriber loop (DSL) and. Tele & Video Conferencing.

Table 3. Pakistan Telecommunication Co. Ltd.

| Data Connectivity Technology | VPN | BANKS |
|------------------------------|-----|-------------------------|
| Digital Cross Connect (DXX) | No | State Bank of Pakistan |
| Digital Cross Connect (DXX) | No | Muslim Commercial Bank |
| Digital Cross Connect (DXX) | No | Askari Commercial Bank |
| Digital Cross Connect (DXX) | No | Standard Chartered Bank |
| Digital Cross Connect (DXX) | No | Union Bank Limited |
| Digital Cross Connect (DXX) | No | Habib Bank Limited |
| Digital Cross Connect (DXX) | No | Bank Alfalah Ltd |
| Digital Cross Connect (DXX) | No | First Women Bank |
| Digital Cross Connect (DXX) | No | Citibank |
| Digital Cross Connect (DXX) | No | American Express Bank |

2.1.2 Virtual Private Network.

Virtual Private Network: which enables your organization to create a private network for interconnection just like a PABX system.

Activate VPN: VPN service is available on exiting telephone lines. One personal Number Plan (PNP) is allotted on each line to subscribe, you just have to quote the numbers (PNPs) required for local and national wide connectivity.

VPN is an (Intelligent Network) IN VPN is an (Intelligent Network) IN service which allows an organization to have private network (local as well as nationwide) using its existing PTCL lines without requiring the installation of dedicated network resources e.g. an organization having sub-offices / branches in the same city or different cities can create a private network on its existing numbers to

communicate with each other just like a PABX system. As the name implies, a Virtual Private Network (VPN) is a virtual network within a real network. [7]

2.1.3 Corporate Customers.

The following organizations can benefit from the PTCL Co-location centers:

ISP's, DSL operators, Premium Rate Services, Data Switches, Web-hosting, Credit Card Authentication System, Band width Provision System, Data-Warehousing Application.

2.2 Multinet Pakistan (Pvt) Ltd.

Multinet is a licensed operator of DSL services on behalf of PTCL. This enables us to install and co-location state-of-the-art, carrier-class DSL equipment at all exchanges (central offices) throughout Pakistan. [8]

At the present time our coverage in Karachi extends to nearly 60% of key business areas of the city Karachi.

Multinet offer the following Services to Corporate Customers:

- 1) *Services: Internet connectivity, VPNs.*
- 2) *Technologies: DSL (Broad Band), HFC (Broad Band), Wireless, SATELLITES*

2.2.1 Technology & protocol use in VPN Communicate:

They proposed to connect different POPs in the Karachi through 128,256 Kbps (or higher bandwidth) DSL links. The circuits will run over ordinary telephone lines and will terminate on their DSLAM'S in the nearest telephone exchange. The circuit will eventually terminate on their backbone network in Karachi.

On this network they provide a VPN an encrypted connection between a user's distributed sites over a public network in this case the individual DSL links are connected to each other via the PTCL ATM network, there fore in order for each POP to communicate with the other, a VPN network would provide a secure, encrypted tunnel.

The encryption mechanism that they use is IPSec and provide security with packet-level encryption.

Table 4. Multinet Pakistan (Pvt) Ltd.

| Data Connectivity Technology | VPNs | BANKS |
|------------------------------|------|--------------|
| DSL+Wireless | No | Fasial Bank |
| DSL+HSDN+Dailup | No | Mezan Bank |
| DSL+Internet | No | Prime Bank |
| DSL+Internet | No | Sonhari Bank |
| DSL+Internet | No | Bolan Bank |

3. DEPLOYING

Deploying a complete Secured Network Model based on VPN Technology solution that would scaleable on a large scale is complex but its implementation will reduce Information Technology Threats and minimize risk on Wide Area Network.

3.1 A Secured Network Model

A Secured Network Model, based on IP Based VPN Technology which can provide all types of security available and its implementation at all levels or Devices and software physical and logical using Layered Approach.

3.1.1 OSI Layered Approach

Table 5. OSI Layered Approach Security View.

| OSI Layers | Security level |
|--------------------|----------------|
| Application Layer | AAA |
| Session Layer | SSL |
| Presentation Layer | Encryptions |
| Transport Layer | Firewalls |
| Network Layer | VPN, IP Sec |
| Data link Layer | MAC Address |
| Physical Layer | Physical |

3.1.2 TCP Layered Approach

Table 6. TCP Layered Approach Security View.

| OSI Layers | Security level |
|-------------------|--------------------------|
| Application Layer | AAA |
| Transport Layer | Firewalls, SSL |
| Network Layer | VPN, IP Sec, Encryptions |
| Data link Layer | MAC Address |
| Physical Layer | Physical |

3.2 IPSec provides security services at the IP Layer

IPSec provides security services at the IP Layer by enabling a system a select required security protocol, determine the algorithms to use for the services and put in place any cryptographic keys required to provide the request services. Two protocols are used to provide security an authentication protocol designated by the header of the protocol, Authentication Header (AH), and a combined encryption authentication protocol designated by the format of the packet for the protocol, Encapsulating Security Payload (ESP).

3.3 IPSec Equipment Infrastructure

IPSec solution can be built using multiple devices Router, Firewall, VPN Client and VPNs concentrators. VPNs solution enabling layered security services.

- 1) *Router*: Some Router integrates VPNs feature, router & firewall offering a complete implementation of IPSec standards.
- 2) *Firewall*: Firewall is high-performance network appliance that provides high-capacity tunnel endpoints with strong firewall feature.
- 3) *VPNs client software*: VPNs client software supports the remote-access VPNs requirement for E-commerce & telecommuting application.
- 4) *VPNs concentrators*:

3.4 The goal of Virtual Private Network

The goal of Virtual Private Network is to simulate a regular network connection to create virtual point-to-point link, any data that is transmitted.

A Virtual Private Network is an enterprise network deployed on a shared infrastructure employing the same security, management, and throughput policies applied in private network.

3.5 Out Tasking VPN Services Management:

Following are IP VPN service management components that businesses might consider out-tasking.

- Managed customer-edge equipment
- Managed network security
- Telecommuter services
- Internet-access integration
- Secure off-net access
- Site-to-site encryption services
- Managed extranet services
- Real-time physical and logical monitoring (event logs, trunk usage, call detail, resource usage, and so on)
- Maintenance of router configuration and upgrades
- Performance management and optimization (circuit availability, network availability, WAN link, router usage)
- Fault identification and resolution with managed backup connectivity for critical sites
- Fault management
- Configuration or change management
- Auditing or asset management
- Performance management
- Network management

CONCLUSIONS

IP-Based VPNs have the capability to offer the best possible availability, QoS, essential security, multicast support and management essential ingredients for a reliable, trouble-free, Scalable network.

REFERENCES

- [1] *Managing Cisco networking security*, Michael J. Wenstrom, Cisco Press, Indianapolis, IN 46290 USA
- [2] *Networking Security Essentials Application & Standards*, William Stallings, Published By Addison Wesley Longman (Singapore)
- [3] RFC 2401: *An Overview of security architecture*
- [4] RFC 2402: *Description of a packet Authentication IP*
- [5] RFC 2406: *Description of a packet Encryption IP*
- [6] RFC 2408: *Specification of key management capabilities*
- [7] Pakistan Telecommunication Company Limited.
- [8] Multinet Broadband Pakistan (Pvt) Ltd.