ISSN No. 0976-5697

Volume 6, No. 3, May 2015 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Connect Users to Private Networks Securely over Public Networks using Virtual Private Networks

Dr. B. BasaweswaraRao
Department of Computer Science and Engineering
Acharya Nagarjuna, University, Guntur
E-mail: bobbabrao@yahoo.co.in

S. Kavitha
Department of Computer Science and Engineering
Acharya Nagarjuna, University, Guntur
E-mail: kavitha.sarihaddu@yahoo.com

***Abstract*:** We propose simple and robust mechanism that an intercepted packet reveal nothing about the true destination system in Virtual Private Networks using tunnel mode and can be used to enable remote offices and users to connect to private networks securely over public networks.

Keywords: virtual private network, network access server (NAS), internet security and acceleration (ISA) server, Point to Point Tunneling Protocol (PPTP), Layer2 Tunneling Protocol(L2TP),or Internet Security Protocol(IPSec)

I. INTRODUCTION

Virtual Private Network (VPN) is a mechanism of creating and controlling a private network over a public network using encryption, authentication and integrity protection. Thus it combines the advantages of a public network with those of private owned network.

A virtual private network is a private and secure network connection between systems that uses the data communication capability of unsecured and public networks. The virtual private network consortium defines a VPN as private data network that make use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol, transport mode, Ipsec and SSLVPN. VPNs are commonly used to extend securely an organization's internal network connections to remote locations.

II. VPN ARCHITECTURE

Using VPNs, an organization can help secure private network traffic over an unsecured network, such as the Internet. VPN helps provide a secure mechanism for encrypting and encapsulating private network traffic and moving it through an intermediate network. Data is encrypted for confidentiality, and packets that might be intercepted on the shared or public network are indecipherable without the correct encryption keys. Data is also encapsulated, or wrapped, with an IP header containing routing information.

There are a number of ways to use VPN. The most common scenario is when a remote user accesses a private network across the Internet using a remote access VPN connection. In another scenario, a remote office connects to the corporate network using either a persistent or an on-demand site-to-site VPN connection (also known as a router-to-router VPN connection).

Each of these VPN scenarios can be deployed to provide connectivity over a public network, such as the Internet, or over a private intranet. VPN connections can also be deployed in an extranet scenario to communicate securely with business partners. An extranet functions as an intranet that can be securely shared with a designated business partner.

With both the remote access and site-to-site connections, VPNs enable an organization to replace long distance dial-up or leased lines with local dial-up or leased lines to an Internet service provider (ISP).

Remote access VPN

A remote access VPN connection is made by a remote access client. A remote access client is a single computer user who connects to a private network from a remote location. The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client. The VPN client authenticates itself to the VPN server and, for mutual authentication, the VPN server authenticates itself to the VPN client.

Site-to-site VPN

A site-to-site VPN connection connects two portions of a private network or two private networks. For example, this allows an organization to have routed connections with separate offices, or with other organizations, over the Internet. A routed VPN connection across the Internet logically operates as a dedicated Wide Area Network (WAN) link.

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India

The VPN server provides a routed connection to the network to which the VPN server is attached. On a site-to-site VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers. The calling router (the VPN client) authenticates itself to the answering router (the VPN server), and, for mutual authentication, the answering router authenticates itself to the calling router.

Internet-based VPN Connections

Using an Internet-based VPN connection, an organization can avoid long-distance charges while taking advantage of the global availability of the Internet.

Remote Access VPN Connections over the Internet

A remote access VPN connection over the Internet enables a remote access client to initiate a dial-up connection to a local ISP instead of connecting to a corporate or outsourced network access server (NAS). By using the established physical connection to the local ISP, the remote access client initiates a VPN connection across the Internet to the organization's VPN server. When the VPN connection is created, the remote access client can access the resources of the private intranet. The following figure shows remote access over the Internet.

VPN Connecting a Remote Client to a Private Intranet

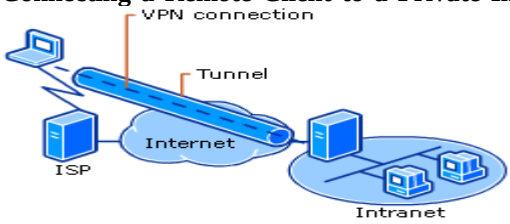


Figure. VPN Connecting a Remote Client to a Private Intranet

Remote Access VPN Connections over an Intranet

In some organization intranets, the data of a department, such as human resources, is so sensitive that the network segment of the department is physically disconnected from the rest of the intranet. While this protects the data of the human resources department, it creates information accessibility problems for authorized users not physically connected to the separate network segment.

VPN connections help provide the required security to enable the network segment of the human resources department to be physically connected to the intranet. In this configuration, a VPN server can be used to separate the network segments. The VPN server does not provide a direct routed connection between the corporate intranet and the separate network segment. The following figure shows remote access over an intranet.

VPN Connection Allowing Remote Access to a Secured Network over an Intranet

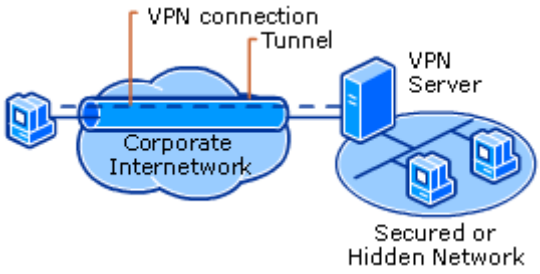


Figure: VPN Connection Allowing Remote Access to a Secured Network over an Intranet

Site-to-Site VPN Connections over an Intranet

Two networks can be connected over an intranet using a site-to-site VPN connection. This type of VPN connection might be necessary, for example, for two departments in separate locations, whose data is highly sensitive, to communicate with each other. For instance, the finance department might need to communicate with the human resources department to exchange payroll information.

The following figure shows two networks connected over an intranet.

VPN Connecting Two Networks over an Intranet

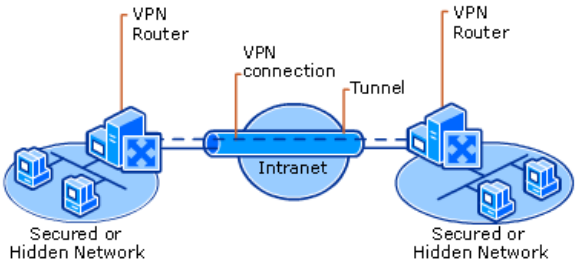


Figure: VPN Connecting Two Networks over an Intranet

the VPN defines three *technologies*: trusted VPNs, Secure VPNs and hybrid VPNs.

1. A trusted VPN also known secure VPNs, uses leased circuits from a service provider and conducts packets switching over these leased circuits. The organization must the service provider, who provides contractual assurance that one else is allowed to use these circuits and that the circuits are properly maintained and protected.

2. Secure VPNs use security protocol and encrypt traffic transmitted across unsecured public networks.

3. Hybrid VPN combines the two, providing encrypted transmissions over all (or) some of a trusted VPN networks.

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India

A VPN that proposes to offer a secure and reliable capability on public networks must accomplish, specific technologies and protocols being used:

- **Encapsulation**: Encapsulation of incoming and outgoing data, where in the native protocol that can be routed over the public network as well as usable by the server network environment.

- **Encryption**: Encryption of incoming data and outgoing data to keep the data content private while in transit over the public network but usable by the client and server computer and / or the local networks on both ends of the VPN connection.

- **Authentication**: Authentication of the remote computer and the remote uses as well.

II-Related Work

There are modes available to VPN. There are:

1. Transport mode
2. Ipsec mode
3. SSL(Secure Socket Layer)VPN mode

In Transport mode, the data within an IP packet is encrypted but the header information is not. This model frequently allows the remote system to act as its own VPN server, which is a weakness.

Ipsec mode can impose high CPU overhead on VPN gateway due to the processing necessary for packet encryption/decryption and authentication.

SSLVPN mode is major security weakness.

We therefore propose the use of Tunnel mode. The primary benefit to this model is that an intercepted packet reveal nothing about the true destination system.

III. TUNNEL MODE

In tunnel mode, the organization establishes two-perimeter tunnel servers. These servers serve as the encryption points, encrypting all traffic that will traverse an unsecured network. In tunnel mode, the entire client packet is encrypted and added as the data portion of a packet addressed from one tunneling server and to another. The receiving server decrypts the packet and sends it to the final address. The primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.

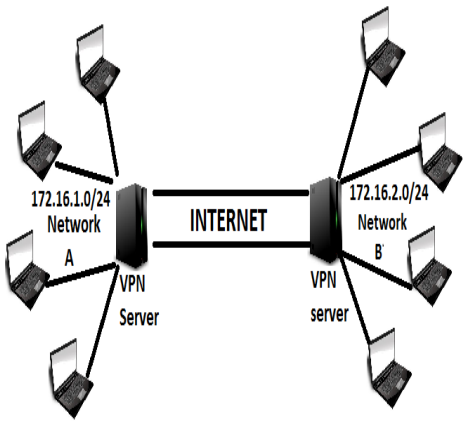


Figure: Tunnel mode VPN

One example of tunnel mode VPN is provided with Microsoft's internet security and acceleration(ISA) server. With ISA server, an organization can establish a gateway-to-gateway tunnel, encapsulating data within the tunnel. ISA can use the Point to Point Tunneling Protocol(PPTP), Layer2 Tunneling Protocol(L2TP),or Internet Security Protocol(IPSec) technologies.

PPTP(Point to Point Tunneling Protocol):

PPTP uses a TCP connection, known as the PPTP control connection, to create, maintain, and terminate the tunnel. PPTP uses a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames as tunneled data. The payloads of the encapsulated PPP frames can be encrypted, compressed, or both.

PPTP assumes the availability of an IP network between a PPTP client (a VPN client using the PPTP tunneling protocol) and a PPTP server (a VPN server using the PPTP tunneling protocol). The PPTP client might already be attached to an IP network that can reach the PPTP server, or the PPTP client might have to use a dial-up connection to a NAS to establish IP connectivity as in the case of dial-up Internet users.

PPTP Control Connection Packet

Data-Link Header	IP	TCP	PPTP Control Message	Data-Link Trailer

PPTP Packet Development

The following figure shows the path that tunneled PPTP data takes through the Windows Server 2003 networking architecture from a VPN client over a remote access VPN connection using an analog modem. The following steps outline this process:

1. An IP datagram is submitted by its appropriate protocol to the virtual interface that represents the

VPN connection using Network Driver Interface Specification (NDIS).

2. NDIS submits the packet to NDISWAN, which encrypts and optionally compresses the data and provides a PPP header consisting of only the PPP Protocol ID field. This assumes that address and control field compression were negotiated during the Link Control Protocol (LCP) phase of the PPP connection process.

3. NDISWAN submits the data to the PPTP protocol driver, which encapsulates the PPP frame with a GRE header. In the GRE header, the Call ID field is set to the appropriate value to identify the tunnel.

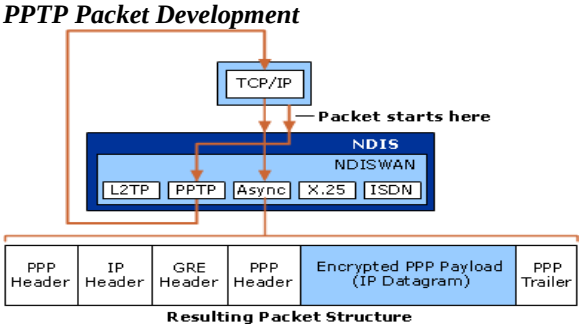
4. The PPTP protocol driver then submits the resulting packet to the TCP/IP protocol driver.

5. The TCP/IP protocol driver encapsulates the tunneled PPTP data with an IP header and submits the resulting packet to the interface that represents the dial-up connection to the local ISP using NDIS.

6. NDIS submits the packet to NDISWAN, which provides PPP headers and trailers.

7. NDISWAN submits the resulting PPP frame to the appropriate WAN miniport driver representing the dial-up hardware (for example, the asynchronous port for a modem connection).

PPTP Packet Development



L2TP (Layer2 Tunneling Protocol)

L2TP encapsulates PPP frames to be sent over IP, X.25, frame relay, or ATM networks. When sent over an IP network, L2TP frames are encapsulated as User Datagram Protocol (UDP) messages. L2TP can be used as a tunneling protocol over the Internet or over private intranets.

L2TP uses UDP messages over IP networks for both tunnel maintenance and tunneled data. The payloads of encapsulated PPP frames can be encrypted or compressed (or both); however, L2TP clients do not negotiate the use of MPPE for L2TP connections. Encryption for L2TP connections is provided by IPSec Encapsulating Security Payload (ESP) in transport mode.

Authentication that occurs during the creation of L2TP tunnels must use the same authentication mechanisms as PPP connections.

L2TP tunnel maintenance and tunneled data have the same packet structure.

IV. SUMMARY

VPN (Virtual Private Network) technology pro
vides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

V. REFERENCES

[1] VPN - Virtual Private Network - Network Security Services-...http://www.vpndynamics.com
[2] Virtual Private Networks, http://www.networkmagazine.com/article/NMG20000727S0029
[3] Virtual Private Networks, http://www.objs.com/survey/vpn.htm
[4] RFC 3145, L2TP Disconnect Cause Information. R. Verma, M. Verma, J. Carlson. July 2001. http://www.ietf.org/rfc/rfc3145.txt
[5] Virtual Private Networks (VPN / PPTP), http://www.wown.com/j_helmig/vpn.htm
[6] Virtual Private Networking, VPN. Secure Virtual Private ..., http://www.securitydogs.com
[7] Tech Guide, Designing and Implementing a Virtual... , http://techguide.zdnet.com/titles/vpnet.shtml
[8] IPsec Implementation Survey, http://web.mit.edu/tytso/www/ipsec/results9710.html
[9] IPsec VPNs With Digital Certificates, http://img.cmpnet.com/internetwk/VPN/graphics/IPsec.pdf
[10] VPN Services, http://global.mci.com/ie/products/vpn/

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India