Virtual Private Network between Remote and Local site using ASA Firewalls

M. Janarandhana Reddy
Dept. E & C
BTLITM, Bangalore -99

Rumana Almas
Dept. E & C
BTLITM, Bangalore -99

Sadiya Kubrha. S
Dept. E & C
BTLITM, Bangalore -99

Ramya. R
Dept. E & C
BTLITM, Bangalore -99

Victor Jeyaseelan D
Dept. E & C
BTLITM, Bangalore -99

Abstract: **The purpose of this project is to provide a more advanced security of ASA Adaptive Security Appliance. The ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. In this project we will be configure the ASA as a basic Firewall with the addition of a third zone referred to as a DMZ and finally we will create a site-to-site VPN between the local and remote sites.**

INTRODUCTION:

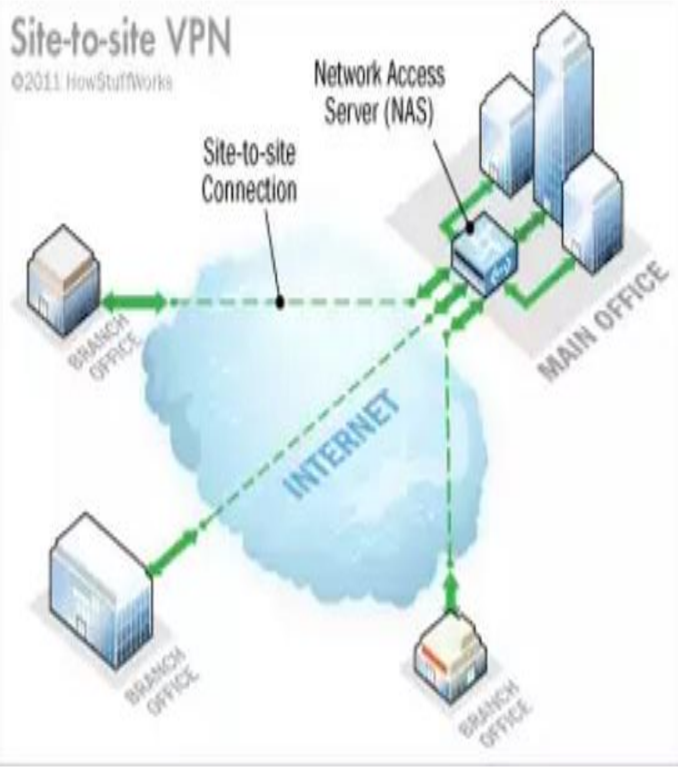
A Virtual Private Network (VPN) connects two computers securely and privately over the internet, even though that is a public network. A VPN client on one computer connects to a VPN server on another computer and by using encryption and other security measures; no-one can see what information is being exchanged.

One use of this technology is to extend a private network across the internet to another location. For example, businesses can enable workers with laptops on the road or at home to connect to the company network as if they were sat at a desk in the office. The network traffic is routed across the internet from the user to the company, but it is encrypted and therefore secure from eavesdropping and interception. A company that has offices in two locations can connect them using a VPN across the

Internet so there appears to be one network. VPNs aren't just for businesses and because the connection is private and secure, another use is to access the internet anonymously. Anyone that wants to protect their privacy and security online should use a VPN. Everywhere online someone is tracking your activities. ISPs monitor internet usage and may restrict the bandwidth if they detect certain activities. P2P file sharing and Bit Torrent traffic is speed-limited for instance. Websites you visit get your IP address, location, browser and operating system, screen resolution, ISP and more.

PROPOSED SOLUTION:

In this project we will be using GNS3 and ASDM to model a network with LOCAL and REMOTE site. Each of these sites will have access to the internet. The local site will also have a DMZ zone that can be access by any outside device as well as inside devices, but will not be able to connect to any inside device. In addition to this we will create a site-to-site VPN between the local site and remote site.



IMPLEMENTATION:

DMZ:

In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical sub network that contains and exposes an organization's external-facing services to a larger and entrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN).an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.

VPN:

VPNs allow employees to securely access their company's intranet while travelling outside the office. Similarly, VPNs securely connect geographically separated offices of an organization, creating one cohesive network. VPN technology is also used by individual Internet users to secure their wireless transactions, to circumvent geo restrictions and censorship, and to connect to proxy servers for the purpose of protecting personal identity and location.

ASA VPN Types:

There are basically three types of VPN available to the Cisco ASA product line they are as follows:

A. Clientless VPN:

Clientless SSL VPN enables end users to securely access resources on the corporate network from anywhere using an SSL-enabled Web browser. The user first authenticates with a Clientless SSL VPN gateway, which then allows the user to access pre-configured network resources.

Clientless SSL VPN creates a secure, remote-access VPN tunnel to an ASA using a Web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of Web resources and both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTP. They include:

- Internal websites.
- Web-enabled applications.
- NT/Active Directory file shares.
- Email proxies, including POP3S, IMAP4S, and SMTPS.
- Microsoft Outlook Web Access Exchange Server 2000, 2003, and 2007.
- Microsoft Web App to Exchange Server 2010 in 8.4(2) and later.
- Application Access (smart tunnel or port forwarding access to other TCP-based applications)

Clientless SSL VPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide the secure connection between remote users and specific, supported internal resources that you configure at an internal server. The ASA recognizes connections that must be proxies, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to resources by users of Clientless SSL VPN sessions on a group basis. Users have no direct access to resources on the internal network.

B. Any Connect VPN:

Cisco Any Connect is an app designed to let you connect securely to VPNs. This is an app for enterprise users who need a secure way to connect to a VPN at their place of work. Coming from a trusted name like Cisco, the app provides a level of safety and security that should be welcome by those who have need of such an app.

C. Site-to-Site VPN:

A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

1) There are two types of site-to-site VPNs:

- Intranet-based -- If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.
- Extranet-based -- When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

Even though the purpose of a site-to-site VPN is different from that of a remote-access VPN, it could use some of the same software and equipment. Ideally, though, a site-to-site VPN should eliminate the need for each computer to run VPN client software as if it were on a remote-access VPN. Dedicated VPN client equipment, described later in this article, can accomplish this goal in a site-to-site VPN.

VPN Tunneling Protocols:

Tunneling enables the encapsulation of a packet from one type of protocol within the datagram of a different protocol. For example, VPN uses PPTP to encapsulate IP packets over a public network, such as the Internet. A VPN solution based on Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), or Secure Socket Tunneling Protocol (SSTP) can be configured. PPTP, L2TP, and SSTP depend heavily on the features originally specified for Point-to-Point Protocol (PPP). PPP was designed to send data across dial-up or dedicated point-to-point connections. For IP, PPP encapsulates IP packets within PPP frames and then transmits the encapsulated PPP-packets across a point-to-point link. PPP was originally defined as the protocol to use between a dial-up client and a network access server.

PPTP:

PPTP allows multiprotocol traffic to be encrypted and then encapsulated in an IP header to be sent across an IP network or a public IP network, such as the Internet. PPTP can be used for remote access and site-to-site VPN connections. When using the Internet as the public network for VPN, the PPTP server is a PPTP enabled VPN server with one interface on the Internet and a second interface on the intranet. Encapsulation PPTP encapsulates PPP frames in IP data grams for transmission over the network. PPTP uses a TCP connection for tunnel management and a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted, compressed, or both. The following figure shows the structure of a PPTP packet containing an IP datagram. Structure of a PPTP Packet Containing an IP Datagram

Structure of a PPTP Packet Containing an IP Datagram

IP Header	GRE Header	PPP Header	PPP payload(IP Datagram)

L2TP:

IP or asynchronous transfer mode (ATM). L2TP is a combination of PPTP and Layer 2 Forwarding (L2F), a technology developed by Cisco Systems, Inc. L2TP represents the best features of PPTP and L2F.Unlike PPTP, the Microsoft implementation of L2TP does not use MPPE to encrypt PPP data grams. L2TP relies on Internet Protocol security L2TP allows multiprotocol traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery, such as (IPSec) in Transport Mode for encryption services. The combination of L2TP and IPSec is known as L2TP/IPSec.

Both L2TP and IPSec must be supported by both the VPN client and the VPN server.

Encapsulation

Encapsulation for L2TP/IPSec packets consists of two layers:

First layer: L2TP encapsulation

A PPP frame (an IP datagram) is wrapped with an L2TP header and a UDP header.

The following figure shows the structure of an L2TP packet containing an IP datagram.

Structure of an L2TP Packet Containing an IP Datagram

IP Header	UDP Header	L2TP Header	PPP Header	PPP Header

Second layer: IPSec encapsulation

The resulting L2TP message is then wrapped with an IPSec Encapsulating Security Payload (ESP) header and trailer, an IPSec Authentication trailer that provides message integrity and authentication, and a final IP header. In the IP header is the source and destination IP address that corresponds to the VPN client and VPN server.

The following illustration shows L2TP and IPSec encapsulation for a PPP datagram.

SSTP:

Secure Socket Tunneling Protocol (SSTP) is a new tunneling protocol that uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPSec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the Secure Sockets Layer (SSL) channel of the HTTPS protocol. The use of PPP allows support for strong authentication methods, such as EAP-TLS. SSL provides transport-level security with enhanced key negotiation, encryption, and integrity checking. When a client tries to establish a SSTP-based VPN connection, SSTP first establishes a bidirectional HTTPS layer with the SSTP server. Over this HTTPS layer, the Protocol packets flow as the data payload. Encapsulation SSTP encapsulates PPP frames in IP data grams for transmission over the network. SSTP uses a TCP connection (over port 443) for tunnel management as well as PPP data frames.

Encryption

The SSTP message is encrypted with the SSL channel of the HTTPS protocol.

Choosing between tunneling protocols

When choosing between PPTP, L2TP/IPSec, and SSTP remote access VPN solutions, consider the following:

PPTP can be used with a variety of Microsoft clients including Microsoft Windows 2000, Windows XP, Windows Vista, and Windows Server 2008. Unlike L2TP/IPSec, PPTP does not require the use of a public key infrastructure (PKI). By using encryption, PPTP-based VPN connections provide data confidentiality (captured packets cannot be interpreted without the encryption key). PPTP-based VPN connections, however, do not provide data integrity (proof that the data was not modified in transit) or data origin authentication (proof that the data was sent by the authorized user).

L2TP can only be used with client computers running Windows 2000, Windows XP, or Windows Vista. L2TP supports either computer certificates or a presaged key as the authentication method for IPSec. Computer certificate authentication, the recommended authentication method, requires a PKI to issue computer certificates to the VPN server computer and all VPN client computers. By using IPSec, L2TP/IPSec VPN connections provide data confidentiality, data integrity, and data authentication.

Unlike PPTP and SSTP, L2TP/IPSec enables machine authentication at the IPSec layer and user level authentication at the PPP layer.

SSTP can only be used with client computers running Windows Vista Service Pack 1 (SP1) or Windows Server 2008. By using SSL, SSTP VPN connections provide data confidentiality, data integrity, and data authentication.

All three tunnel types carry PPP frames on top of the network protocol stack. Therefore, the common features of PPP, such as authentication schemes, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPV6) negotiations, and

Network Access Protection (NAP), remain the same for the three tunnel types.

***ASDM*:**
ASDM is a GUI-Based Firewall Appliance Management tool that is user friendly and allows the user to configure, monitor, and troubleshoot Cisco firewall appliances and firewall service modules. Ideal for small or simple deployments, the Cisco Adaptive Security Device Manager provides the following:

- Setup wizards that help you configure and manage Cisco firewall devices, including the ASA Adaptive Security Appliances, Cisco PIX appliances, and Catalyst Series Firewall Services Modules without cumbersome command-line scripts
- Powerful real-time log viewer and monitoring dashboards that provides an at-a-glance view of firewall appliance status and health
- Handy troubleshooting features and powerful debugging tools such as packet trace and packet capture.

REQUIREMENTS:

A. SOFTWARE REQUIREMENT:

a.	SOFTWARE:	: GNS3
b.	OPERATING SYSTEM	: Windows 7

B. HARDWARE REQUIREMENT:

a.	Hard Disk	: 1GB
b.	RAM	: 2GB

FUTURE IMPLEMENTATION:

We can develop a vpn system such that we would able to find the original MAC Address of the hacker and also exact geographical location of that hacker. And also by adding additional layers of security protocols we can still able to provide high security and better privacy.

CONCLUSION:

Only authorized person can take an access of the network and complete network will be handling by the network administration, so the network will be safe because network administration person can make a change in network.

REFERENCES:

[1] RFC 3415,L2TP Disconnect cause information. R.Verma,M.Verma,J.Carlson.july 2001 http://www.ietf.org/rfc/rfc3145.txt
[2] RFC 3093, firewall enhancement protocol(FEP).M.Gaynor,s.Bradner.1 April 2001. http://www.ietf.org/rfc/rfc3093.txt
[3] RFC 2888,secure remote access L2TP .p.Srisuresh.August 2000 http://www.ietf.org/rfc/rfc2888.txt
[4] RFC 2685,virtual private network identifier.B.fox,B.Gleeson.September 1999 http://www.ietf.org/rfc/rfc2685.txt
[5] RFC 2663,IP Network address translator(NAT) teterminolgy and consideration .P.Srisuresh,M. Holdrege.August 1999. http://www.ietf.org/rfc/rfc2663.txt
[6] RFC 2637 .Point-2-point tunnenling protocol.K.Hamzeh,G. Pall,W. Verthein,j. Taarud,W.Little,G.Zorn.july 1999 http://www.ietf.org/rfc/rfc2637.txt