Global Information Assurance Certification Paper

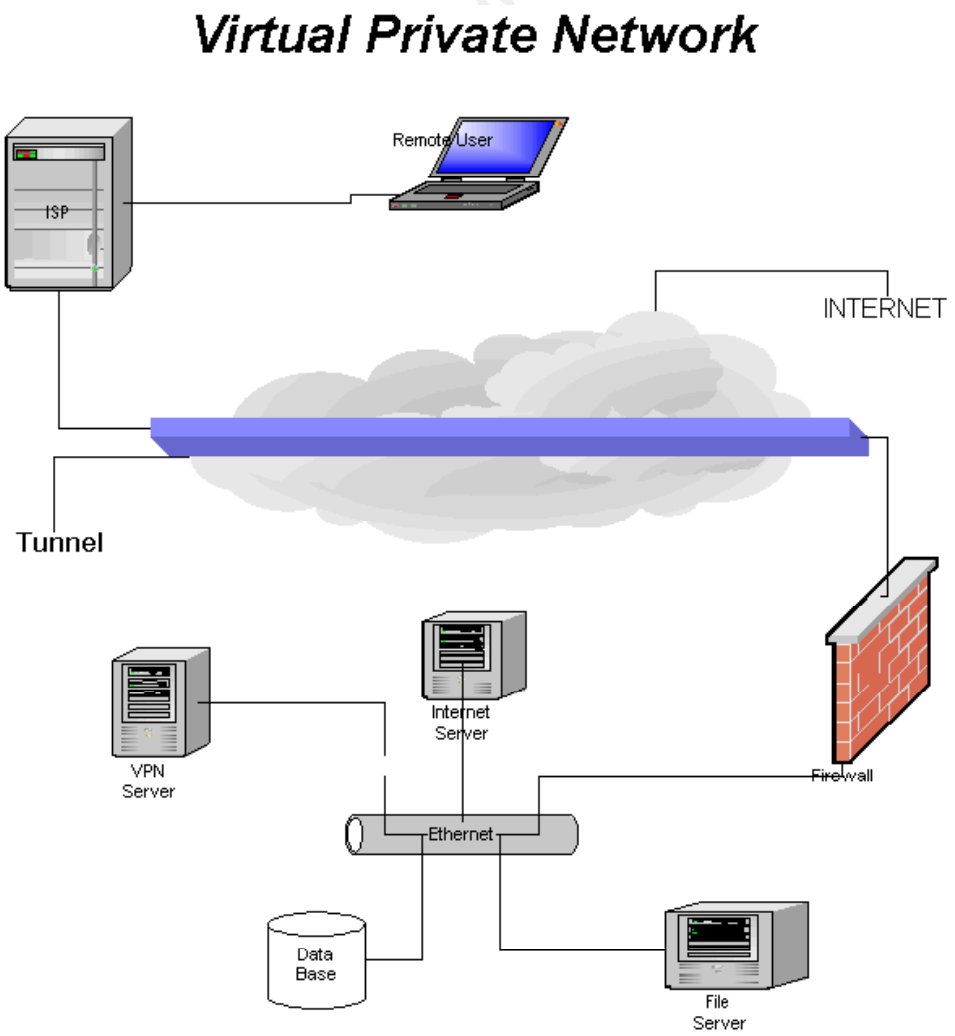
Virtual Private Network (VPN) Security

Gregory J. Ciolek
January 4, 2001

Introduction
This paper is intended to present to you how a VPN deals with the basic Internet security concerns.

1: Authentication – The ability to verify the parties on both ends of the link.
2: Integrity – The ability to verify that all data transmitted and received has not been tampered with or changed.
3: Confidentiality – The ability to ensure that all transmitted data over the link is not read or intercepted by unauthorized individuals.

A VPN is a combination of software and hardware that allows telecommuters, remote sites and business partners to use the Internet to establish a secure connection with a host network. This connection forms what appears to be a private network. Below is an example of a VPN.



A secure connection is established by tunneling through the Internet. Tunneling is the encapsulation of a message packet within an IP (Internet Protocol) packet for transmission across the Internet. The encapsulated packet is striped from the IP packet at the receiving network. There are three protocols for tunneling through the Internet, Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP) and Point to Point Tunneling Protocol (PPTP). All three protocols adhere to the basic Internet security standards.

Internet Protocol Security (IPSec)
IPSec is part of the IP (Internet Protocol) protocol group. It provides two protocols called AH (Authentication header) and ESP (Encapsulated Security Payload). AH and ESP provide for authentication, integrity and confidentiality when using IPSec.
The AH header comes right after the IP Header and contains cryptographic hashes of data and identification. The AH protects the source and destination addresses of the IP header. The ESP header allows for encryption of the data payload protecting data privacy and integrity. ESP works with symmetric encryption algorithms: DES, 3DES and Blowfish. In order to use IPSec you have to use the same protocols, encryption algorithms and keys on both sides of the connection.
The IPSec protocol combines key management with support for digital certificates. IPSec supports the use of Internet Key Exchange (IKE) which is a method for exchanging secure encryption keys over the Internet.

Point to Point Tunneling Protocol (PPTP)
PPTP was developed by Microsoft, Ascend, 3Com, US Robotics and ECI Telematics. The majority of PPTP clients use the Microsoft version of PPTP. PPTP achieves user authentication by using Extensible Authentication Protocol (EAP), Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), CHAP, Shiva Password Authentication Protocol (SPAP) and Password Authentication Protocol (PAP). All five of these protocols rely on the strength of the password. A strong password policy is one of the simplest means to accomplish authentication and security. Here is an example of a Strong password policy.

Every regular user will be required to enter a unique password for network access.
Attributes of passwords:

- must be between 6 and 8 characters
- contain at least one lowercase alphabetic character, one uppercase alphabetic character and one numeric digit
- cannot contain consecutive characters
- cannot match any of the past eight passwords
- cannot contain user name
- will be changed every 60 days
- should not be easily guessed or crackable.

Accounts are locked out after three failed sign-on attempts.
Password strength will be tested periodically, some users may be asked to change their passwords to something more complex.

PPTP encapsulates PPP frames into IP data-grams for transmission over the Internet using a modified version the Generic Routing Encapsulation (GRE).

Encryption in PPTP is handled by using Microsoft Point-to-Point Encryption (MPPE). MPPE provides only link encryption and in Windows 2000 you have to use EAP or MS-CHAP in order to encrypt PPTP payloads. MPPE uses the RSA RC4 stream cipher for 40-bit, 56-bit & 128-bit encryption.

Layer Two Tunneling Protocol (L2TP)
L2TP is a combination of PPTP and Layer 2 Forwarding (L2F) developed by Cisco Systems. Tunneling using L2TP is accomplished through multiple levels of encapsulation: L2TP, UDP, IPSec, IP, and Data-Link.
L2TP can authenticate the user and the computer. Computer authentication in L2TP is done through an IPSec ESP connection using computer certificates. The certificate identifies the computer itself and not the person using the computer. User authentication is done through a PPTP connection using MS-CHAP, CHAP, SPAP and PAP.
Encryption is accomplished through the use of L2TP over IPSec using DES and 3DES.

Firewalls
Integrity can be strengthened in a VPN by the use of a Firewall. There are three approaches to the use of a firewall with a VPN server. Place the firewall between the Internet and the VPN server, corporate network. Place the firewall between the VPN and the corporate network. Place the VPN parallel to an existing firewall.
The diagram on page 1 shows the firewall in front of the VPN server.
The easiest method is to place the VPN parallel to an existing firewall, since it will require no changes to the firewall. The big drawback being you open up two entry points to your network.
Placing the VPN behind an existing firewall requires you to make changes to the firewall. You will have to configure it to filter VPN traffic. It should be noted that not all firewalls have the ability to filter VPN traffic.
Placing the VPN in front of the firewall is said to be the securest method. The VPN can be configured to filter out non-VPN traffic and pass it through to the firewall. The VPN is then left to authenticate and decrypt VPN traffic. VPN traffic is then passed to the firewall for further filtering and routing.
You could also place the VPN on the same server as the firewall, but with two processor intensive applications running on the same server it would slow your network down.

Authentication Re-enforcement's
Authentication in a VPN can also be enhanced by the use of Smart Cards and Token Cards. The only consideration to these methods of security is funding.

Smart Cards
Smart cards are small devices about the size of a credit card. They contain a rudimentary CPU and memory chip. They are used to store user profile, encryption keys and algorithms. They usually require a PIN number in order to use them.

Token Cards
Token cards are similar to Smart cards in that they are about the same in size. They will usually have a small LCD display and a keypad. The user enters a PIN number and the card will then display a passcode, which is used to gain access to the network. all three are very good means at establishing authentication with cost probably being the one deciding factor.

Remote Authentication Dial-In User Service (Radius Servers)
A RADIUS server is a central authentication database. It maintains a profile of the users of the VPN. It can maintain a users connection parameters, IP address assignments, callback information time allotments and accounting information

To wrap up on how a VPN meets security concerns of Internet usage, Authentication, Integrity and Confidentiality.

Authentication
Authentication in **IPSec** with the AH and ESP headers.
Authentication in **PPTP** when passwords are authenticated.
Authentication in **L2TP** is provided by the use of IPSec and PPTP.

Integrity
With **IPSec** integrity is managed by the AH header which secures the source and destinations portions of the IP header. The ESP protocol also provides integrity from the anti-replay services.
The **PPTP** protocol assures integrity by tightly coordinating the packet flow.
L2TP through the use of IPSec and PPTP maintains integrity in the same manner.

Confidentiality
The basis for maintaining confidentiality in all three protocols is through the use of encryption. All three protocols provide strong encryption by using DES, DES3& RSA RC4.

Sources:

Microsoft White Paper, Virtual Private Networks An Overview
http://www.microsoft.com/WINDOWS2000/Library/howitworks/communications/remoteaccess/vpnoverview.asp 1999

Microsoft White Paper, Virtual Privacy Protected Network Access: Virtual Private Networking and Intranet Security
http://www.microsoft.com/WINDOWS2000/Library/howitworks/communications/remoteaccess/nwpriv.asp 1999

Securing L2TP using IPSEC, INTERNET-DRAFT Category: Standards Track
Baiju, Patel: Bernard, Aboba: Microsoft, 2 February 1999
http://www.ietf.org/proceedings/99mar/I-D/draft-ietf-pppext-l2tp-security-03.txt

The Point-to-Point Protocol (PPP)
Network Working Group W. Simpson, Editor Request for Comments: 1661 Daydreamer
STD: 51 July 1994 Obsoletes: 1548 Category: Standards Track
http://www.ietf.org/rfc/rfc1661.txt?number=1661

Security Architecture for the Internet Protocol
Network Working Group Request for Comments: 2401 Obsoletes: 1825 Category: Standards Track, BBN Corp, S. Kent, R. Atkinson @Home Network, November 1998
http://www.ietf.org/rfc/rfc2401.txt?number=2401

IP Security Document Roadmap
Network Working Group, Request for Comments: 2411 Category: Informational
N. Doraswamy, R. Thayer, Bay Networks, R. Glenn, NIST, Sable Technology Corporation, November 1998
http://www.ietf.org/rfc/rfc2411.txt?number=2411

Virtual Private Networks: Foundation and Practical How-To's
SANS2000 Course Book, Tina Bird, March 23,2000

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS